Citrix® Password Manager-Installationshandbuch

Citrix Password Manager™ 4.6
Citrix Presentation Server™ 4.5 mit Feature Pack 1, Platinum Edition

Hinweise zu Copyright und Marken

Die Verwendung des in diesem Handbuch beschriebenen Produkts unterliegt der Annahme der Endbenutzerlizenzvereinbarung. Eine druckbare Kopie der Endbenutzerlizenzvereinbarung finden Sie auf der Produkt-CD.

Die in diesen Unterlagen enthaltenen Angaben und Daten können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Firmen, sonstigen Namen und Daten sind frei erfunden, sofern nichts anderes angegeben ist. Ohne ausdrückliche schriftliche Erlaubnis von Citrix Systems, Inc. darf kein Teil dieser Unterlagen für irgendwelche Zwecke vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, weder elektronisch noch mechanisch.

Citrix Password Manager ersetzt die Verschlüsselungsschlüssel bestimmter Endbenutzer bei jedem Wechsel der primären Authentifizierungsmethode, z. B. Ändern des Domänenkennworts oder Ausstellen einer neuen Smartcard. Password Manager kann mit dem optionalen Schlüsselverwaltungsmodul diesen Vorgang automatisch ausführen. Password Manager kann auch die Microsoft Data Protection API (DPAPI) verwenden. Bei Verwendung des optionalen Schlüsselverwaltungsmoduls und/oder von DPAPI kann ein Administrator auf die in Password Manager gespeicherten Anmeldeinformationen des Benutzers für das Unternehmen oder den Privatgebrauch zugreifen, wenn sich der Administrator als dieser Endbenutzer anmeldet. Für zusätzliche Sicherheit wird möglicherweise die Identität der Endbenutzer mit eindeutigen vom Benutzer bereitgestellten Informationen geprüft. Dies stellt ein zusätzliches Sicherheitsniveau für die sekundären Anmeldeinformationen des Benutzers bereit.

Regionale Gesetzesvorschriften zum Benutzercomputing schreiben möglicherweise vor, dass Sie Endbenutzer auf die möglichen Sicherheits- und Datenschutzauswirkungen hinweisen, die eine Bereitstellung des Schlüsselverwaltungsmoduls und der DPAPI-Sicherheitskonfigurationen haben können. Prüfen Sie die Unternehmensrichtlinien und legen Sie fest, welche Benachrichtung ggf. für die Endbenutzer benötigt wird.

© 2003-2007 Citrix Systems, Inc. Alle Rechte vorbehalten.

v-GO code © 1998-2003 Passlogix, Inc. Alle Rechte vorbehalten.

Citrix, ICA (Independent Computing Architecture) und Program Neighborhood sind eingetragene Marken; Citrix Presentation Server, Citrix Password Manager und SpeedScreen sind Marken von Citrix Systems, Inc. in den USA und anderen Ländern.

RSA Encryption © 1996-1997 RSA Security Inc. Alle Rechte vorbehalten.

Dieses Produkt enthält Software, die von The Apache Software Foundation (http://www.apache.org/) entwickelt wurde.

Dieses Produkt enthält Software, die von Salamander Software Ltd entwickelt wurde. © 2002 Salamander Software Ltd. Parts © 2003 Citrix Systems, Inc. Alle Rechte vorbehalten.

Lizenzierung: Teile dieser Dokumentation über Globetrotter, Macrovision und FLEXlm sind urheberrechtlich geschützt von © 2003-2006 Macrovision Corporation und/oder Macrovision Europe Ltd.

Anerkennung von Marken

Adobe, Acrobat und PostScript sind Marken oder eingetragene Marken von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Java, Sun und SunOS sind Marken oder eingetragene Marken von Sun Microsystems, Inc. in den USA und anderen Ländern. Solaris ist eine eingetragene Marke von Sun Microsystems, Inc., die dieses Produkt nicht getestet oder anerkannt haben.

Teile dieser Software basieren partiell auf der Arbeit der Independent JPEG Group.

Teile dieser Software enthalten Imagingcode, der Eigentum und Copyright von Pegasus Imaging Corporation, Tampa, FL ist. Alle Rechte vorbehalten.

Macromedia und Flash sind Marken oder eingetragene Marken von Macromedia, Inc. in den USA und anderen Ländern.

Microsoft, MS-DOS, Windows, Windows Vista, Windows Media, Windows Server, Windows NT, Win32, Outlook, ActiveX, Active Directory und DirectShow sind eingetragene Marken oder Marken von Microsoft Corporation in den USA und/oder anderen Ländern.

Netscape und Netscape Navigator sind eingetragene Marken von Netscape Communications Corp. in den USA und anderen Ländern.

Novell Directory Services, NDS und NetWare sind eingetragene Marken von Novell, Inc. in den USA und anderen Ländern. Novell Client ist eine Marke von Novell, Inc.

RealOne ist eine Marke von RealNetworks, Inc.

Lizenzierung: Globetrotter, Macrovision und FLEXlm sind Marken und/oder eingetragene Marken von Macrovision Corporation.

Alle anderen Marken und eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber.

Dokumentcode: 4. September 2007 (rcw)

Inhalt

Kapitel 1 Willkommen

Password Manager-Komponenten 8
Password Manager-Produktlinie 11
Password Manager Advanced Edition 11
Password Manager Enterprise Edition 12
Informationen zu diesem Dokument 13
Zielgruppe und Annahmen 13
Feedback zu diesem Handbuch 13
Dokumentationskonventionen 14
Weitere Informationen und Support 15
Produktdokumentation 15
Kundendienst und technischer Support 17
Subscription Advantage 18
Schulung und Zertifizierung 18

Kapitel 2 Planen der Password Manager-Umgebung

Diagramm des Planungsablaufs 20
Erste Schritte 21
Auswählen des Typs des zentralen Speichers 23
Auswählen von Active Directory als zentralen Speicher 25
Auswählen einer NTFS-Netzwerkfreigabe 27
Auswählen eines freigegebenen Novell Ordners 29
Verwenden der Kontozuordnung mit mehreren zentralen Speichern und Kontoanmeldeinformationen der Benutzer in einem Unternehmen mit mehreren Domänen 30
Verwenden von Kennwortrichtlinien für den Zugriff auf Anwendungen 33
Standardkennwortrichtlinie 33
Domänenkennwortrichtlinie 34
Benutzerdefinierte Kennwortrichtlinien 34
Überlegungen 35
Standardeinstellungen für die Standardrichtlinie und die Domänenrichtlinie . . 36

Typen der im Unternehmen verwendeten Single Sign-On-aktivierten Anwendungen. 39
Benötigte Informationen zu den Anwendungen 40
Typen der im Unternehmen verwendeten Smartcards 42
Smartcard-Unterstützung 42
Softwareanforderungen für Smartcards 43
Verwenden der Identitätsprüfung 44
Prüfen der Benutzeridentität mit Sicherheitsfragen (fragenbasierte Authentifizierung). 46
Automatisches Wiederherstellen oder Aufheben der Sperrung der Anmeldeinformationen des Benutzers. 47
Planen der Benutzerkonfigurationen 48
Überlegungen 50
Gemeinsames Verwenden von Ressourcen oder Arbeitsstationen (Hotdesktop) . 51
Steuern von Anwendungen. 52
Benutzererfahrung bei Hotdesktop. 52
Lizenzierungsanforderungen 54
Getrennter Modus 54
Verwalten einer Umgebung mit gemischten Lizenztypen. 55
Auswählen optionaler Funktionen des Password Manager-Dienstes 57
Konto-Self-Service 58
Datenintegrität. 59
Schlüsselverwaltung 60
Provisioning 61
Synchronisierung der Anmeldeinformationen (Kontozuordnung) 62
Bereitstellungsszenarios für Password Manager Agent 63
Überlegungen zu Presentation Server 64
Richtlinien für mehrere primäre Authentifizierungsmethoden und Methoden zum Schutz der Anmeldeinformationen der Benutzer 65
Dialogfeld „Datenschutzmethoden“. 65
Dialogfeld „Sekundäre Datenschutzmethode“ 66
Sicherheit und Benutzerfreundlichkeit. 66
Annahme der Identität des Benutzers. 67
Benutzername und Kennwort. 68
Smartcards mit Zertifikaten und Authentifizierungsdaten der Benutzer. 69
Smartcards mit PINs. 71
Servergespeicherte Profile (Microsoft DPAPI) 72
Leere Kennwörter 74

Kapitel 3 Installieren von Password Manager

Zusammenfassung der Installationsschritte 76
Hardware- und Softwareanforderungen 77
Erforderliche unterstützende Systemsoftware 77
Anforderungen für die Password Manager Console und Password Manager Agent 78
Anforderungen für den Password Manager-Dienst 80
ASP.NET-Anforderungen 80
Sicherheits- und Kontoanforderungen für den Password Manager-Dienst 81
Anforderungen für das Serverauthentifizierungszertifikat 81
Erforderliche Konten für Dienstmodule 83
Kontoanforderungen zum Installieren und Verwenden von Password Manager . . 86
Installieren und Verwenden des Password Manager-Dienstes 86
Installieren und Verwenden der Password Manager Console und des Anwendungsdefinitionstools 86
Installieren und Verwenden von Password Manager Agent 87
Installieren von Microsoft .NET 2.0 Framework 88
„Side-by-Side“-Installation von .NET 2.0 und .NET 1.1 88
Installieren von Java Runtime Environment 90
Installieren oder Aktualisieren von JRE nach der Installation der Konsole, des Anwendungsdefinitionstools oder der Agentsoftware 90
Problembehandlung bei Java-bezogenen Fehlermeldungen beim Installieren oder Deinstallieren der Agentsoftware 91
Lizenzierungsanforderungen 92
Vor der Installation von Password Manager 93
Installationsreihenfolge 94
Installationsort der einzelnen Komponenten von Password Manager 95
Erstellen eines zentralen Speichers 96
Erstellen eines zentralen Speichers an einer Befehlszeile (optional) 99
Erstellen eines zentralen Speichers unter Active Directory 100
Erstellen eines zentralen Speichers auf einer NTFS-Netzwerkfreigabe 102
Erstellen eines zentralen Speichers in einem freigegebenen Novell Ordner . . 104
Installieren und Konfigurieren des Password Manager-Dienstes 106
Portnummer für den Password Manager-Dienst 112
Installieren und Konfigurieren der Password Manager Console 113
Installieren und Konfigurieren von Password Manager Agent 117
Installationsszenarios 119
Konfigurieren und Verwenden der Mehrdomänendienstfunktion 129
Anforderungen 129
Taskübersicht 131

Kapitel 4 Aktualisieren von Password Manager

Unterstützte Upgradepfade 134
Zusammenfassung der Upgrade-Schritte. 134
Vor dem Upgrade von Password Manager 135
Verwenden von Autorun 136
Upgradereihenfolge 136
Verwenden des Tools CtxMoveKeyRecoveryData zum Sichern von Dienstdaten 137
Sichern der Datei process.xml (nur in Hotdesktop-Umgebungen) 138
Sichern des vorhandenen zentralen Speichers 138
Aktualisierte Richtlinien, Anwendungsdefinitionen, Fragen/Fragenkataloge und Benutzerkonfigurationen 139
Microsoft .NET Version 1.1 und 2.0 140
Schritt 1: Aktualisieren des Password Manager-Dienstes. 141
Schritt 2: Aktualisieren der Password Manager Console 143
Schritt 3: Aktualisieren von Password Manager Agent 146

Willkommen

Citrix Password Manager stellt Kennwortsicherheit und Single Sign-On-Zugriff auf Windows-Anwendungen, Webanwendungen und hostbasierte Anwendungen bereit, die in der Citrix Umgebung oder auf dem Desktop ausgeführt werden. Benutzer werden einmal authentifiziert, und Password Manager führt alle anderen Vorgänge aus, d. h. Anmeldung an jedem durch Kennwort geschützten Informationssystem, Einhaltung der Kennwortrichtlinien und Überwachung aller mit Kennwörtern verbundenen Ereignisse. Selbst Endbenutzeraufgaben, u. a. Kennwortänderungen, werden automatisiert.

In diesem Dokument, dem *Citrix Password Manager-Installationshandbuch*, finden Sie die Informationen, die für das Planen und Ausführen der Installation von Password Manager 4.6 oder dem Upgrade der vorhandenen Version von Password Manager auf Password Manager 4.6 benötigt werden.

In diesem Abschnitt wird Folgendes beschrieben:

- „Password Manager-Komponenten“ auf Seite 8
- „Password Manager-Produktlinie“ auf Seite 11
- „Informationen zu diesem Dokument“ auf Seite 13
- „Weitere Informationen und Support“ auf Seite 15

Password Manager-Komponenten

In den folgenden Abschnitten werden die Komponenten beschrieben, die Sie für die Installation von Password Manager benötigen. Weitere Informationen finden Sie unter „Planen der Password Manager-Umgebung“ auf Seite 19.

Password Manager besteht aus den folgenden Hauptkomponenten:

- **Zentraler Speicher:** Der zentrale Speicher ist ein zentrales Repository, das in Password Manager zum Speichern und Verwalten von Benutzerdaten und administrativen Daten verwendet wird. Benutzerdaten sind zum Beispiel die Anmeldeinformationen der Benutzer, Antworten auf Sicherheitsfragen und andere auf Benutzer bezogene Daten. Administrative Daten sind zum Beispiel Kennwortrichtlinien, Anwendungsdefinitionen, Sicherheitsfragen und andere allgemeine Daten. Wenn sich ein Benutzer anmeldet, vergleicht Password Manager die Anmeldeinformationen des Benutzers mit den Daten im zentralen Speicher. Wenn der Benutzer kennwortgeschützte Anwendungen oder Webseiten öffnet, werden die aktuellen Anmeldeinformationen aus dem zentralen Speicher abgerufen.

- **Password Manager Console:** Die Password Manager Console ist das Befehlszentrum von Password Manager. In der Konsole können Sie das Verhalten von Password Manager für die Benutzer anpassen. Hier konfigurieren Sie die Funktionsweise von Password Manager, die bereitgestellten Funktionen, die verwendeten Sicherheitsmaßnahmen und weitere wichtige Einstellungen zum Kennwortschutz.

  Die Konsole enthält im linken Bereich vier Objekte oder Knoten. Durch Auswählen eines Knotens werden die Tasks für diesen Knoten angezeigt. Es gibt die folgenden Knoten:

  - Benutzerkonfigurationen: Mit diesen Konfigurationen können Sie bestimmte Einstellungen für Benutzer anpassen, die auf den geografischen Standorten oder den Unternehmensrollen der Benutzer basieren. Mit den Einstellungen der anderen drei Knoten werden Benutzerkonfigurationen erstellt.

  - Anwendungsdefinitionen: Diese Definitionen stellen die Informationen bereit, damit die Agentsoftware die Anmeldeinformationen an die Anwendungen senden und auftretende Fehlerzustände erkennen kann. Sie können die Anwendungsdefinitionsvorlagen verwenden, die mit Password Manager ausgeliefert werden, um Zeit zu sparen, oder Sie können benutzerdefinierte Definitionen für Anwendungen erstellen, die diese Vorlagen nicht verwenden können. Weitere Vorlagen finden Sie unter http://www.citrix.com/passwordmanager/gettingstarted.

- Kennwortrichtlinien: Diese Richtlinien steuern die Kennwortlänge, den Typ und die Zeichenvielfalt, die in benutzerdefinierten und automatisch generierten Kennwörtern verwendet werden. In Kennwortrichtlinien legen Sie auch fest, welche Zeichen nicht in Kennwörtern verwendet werden dürfen, und ob alte Kennwörter wieder verwendet werden dürfen. Durch das Erstellen von Kennwortrichtlinien gemäß der Sicherheitsrichtlinien Ihres Unternehmens stellen Sie sicher, dass die Kennwortsicherheit von Password Manager richtig verwaltet wird.
- Identitätsprüfung: Die von Ihnen erstellten Sicherheitsfragen stellen der Agentsoftware ein zusätzliches Sicherheitsniveau bereit, da sie vor Personifikationen und unberechtigten Kennwortänderungen schützen. Benutzer, die sich registrieren und die Sicherheitsfragen beantworten, können die Identität bestätigen, indem sie dieselben Antworten eingeben. Nach der Prüfung können die Benutzer die Self-Service-Tasks für ihr Konto durchführen, z. B. Zurücksetzen des primären Kennworts oder Aufhebung der Kontosperrung. Die Sicherheitsfragen werden auch für die Schlüsselwiederherstellung verwendet.

- **Password Manager Agent-Software:** Password Manager Agent ist die Software, die zur Vermittlung zwischen den Benutzern und den Anwendungen auf den Clientgeräten der Benutzer installiert sein muss. Password Manager Agent sendet die entsprechenden Anmeldeinformationen an die Anwendungen, die auf dem Clientgerät des Benutzers ausgeführt werden, erzwingt die Kennwortrichtlinien, stellt die Self-Service-Funktion bereit und ermöglicht das benutzerseitige Verwalten der Anmeldeinformationen mit dem Anmeldungsmanager.

- **Password Manager-Dienst:** Der Password Manager-Dienst wird auf einem Webserver ausgeführt, der das Fundament für optionale Funktionen bereitstellt, die in diesem Releases enthalten sind. Installieren Sie den Password Manager-Dienst, wenn Sie mindestens eines der folgenden Module implementieren möchten:
    - Konto-Self-Service: Ermöglicht das benutzerseitige Zurücksetzen der Windows-Kennwörter und das Aufheben der Sperrung der eigenen Windows-Konten.
    - Datenintegrität: Schützt die Daten bei der Übertragung vom zentralen Speicher zum Agent vor Manipulation.
    - Schlüsselverwaltung: Mit dieser Funktion können Benutzer bei einer Änderung des primären Kennworts die sekundären Anmelde-informationen wiederherstellen, entweder mit der automatischen Schlüsselwiederherstellung oder durch das Beantworten von Sicherheitsfragen mit der fragenbasierten Authentifizierung.
    - Provisioning: Ermöglicht das Hinzufügen, Entfernen oder Aktualisieren von Benutzerdaten und Anmeldeinformationen von Password Manager in der Konsole.
    - Synchronisierung der Anmeldeinformationen: Synchronisiert die Anmeldeinformationen der Benutzer über einen Webdienst.

Password Manager-Produktlinie

Password Manager ist jetzt in zwei Editionen erhältlich:

- Password Manager Advanced Edition
- Password Manager Enterprise Edition

Außerdem enthält Citrix Presentation Server 4.5 mit Feature Pack 1, Platinum Edition, eine Funktion „Single Sign-On Powered by Password Manager“, die mit Password Manager Enterprise Edition vergleichbar ist.

Password Manager Advanced Edition

Die Password Manager Advanced Edition erhöht die Sicherheit Ihres Unternehmens durch folgende Funktionen:

- Optionen für starke Kennwortrichtlinien
- Automatische Kennwortgenerierung
- Option zum automatischen Starten des Assistenten für Kennwortänderungen
- Kennwortverschlüsselung bei Speicherzugriff und Übertragung
- Optionen zum Kennwortablauf für Anwendungen ohne entsprechende Funktion

Die Advanced Edition arbeitet auch gut mit anderen Programmen zusammen, wodurch das Speichern der Anmeldeinformationen für den Benutzer und die Verwaltung dieses Vorgangs und dieser Daten für Sie erleichtert wird.

Password Manager Enterprise Edition

Password Manager Enterprise Edition ist für sehr anspruchsvolle und komplexe Unternehmensumgebungen konzipiert. Die Enterprise Edition bietet folgende Vorteile:

- Zusätzliche Sicherheitsfunktionen, Self-Service-Funktionen und Benutzermobilitätsfunktionen für mobile Mitarbeiter im Unternehmen sowie höhere Leistung
- Weniger Helpdeskanrufe durch Self-Service-Funktionen, mit denen die Benutzer ihre Windows-Kennwörter selbst ändern und die Sperrung ihrer Konten selbst aufheben können
- Schneller Zugriff auf Daten für mobile Mitarbeiter im Unternehmen mit Hotdesktop, schnelles Wechseln zwischen Benutzern auf gemeinsam genutzten Arbeitsstationen
- Sicherheitsfunktionen für Unternehmen, wie z. B. Integration von Smartcards, Kerberos und Federated Environment Support (ADFS und SAML).

Informationen zu diesem Dokument

Dieses Handbuch soll Ihnen Folgendes vermitteln:

- Eine Übersicht der Voraussetzungen und Schritte, die für eine erfolgreiche Installation von Password Manager benötigt werden.
- Richtlinien zur Planung und Implementierung einer Bereitstellung von Password Manager im Unternehmen.
- Anweisungen und Tipps zum Erstellen und Beibehalten der optimalen Kennwortverwaltungsumgebung für die Benutzer

Zielgruppe und Annahmen

Dieses Dokument wendet sich an System- und Sicherheitsadministratoren, die Password Manager-Versionen installieren oder aktualisieren. Grundkenntnisse zur Windows Server-Administration werden vorausgesetzt. Sie müssen mit Novell NetWare vertraut sein, wenn Sie Password Manager auf dieser Plattform installieren oder verwalten.

Feedback zu diesem Handbuch

Um Feedback zur Dokumentation zu geben, gehen Sie auf http://www.citrix.com und klicken Sie auf **Support** > **Knowledge Center** > **Product Documentation**. Klicken Sie auf den Link **Submit Documentation Feedback**, um das Feedbackformular aufzurufen.

Dokumentationskonventionen

Die Citrix Produktdokumentation verwendet die folgenden typografischen Konventionen für Menüs, Befehle, Tasten und Objekte in der Benutzeroberfläche des Programms:

Konvention	Bedeutung
Fettdruck	Befehle, Namen von Benutzeroberflächenobjekten, z. B. Textfelder und Optionsschaltflächen, sowie Benutzereingaben.
Kursiv	Platzhalter für Informationen oder Parameter, die Sie eingeben müssen. *Dateiname* in einem Verfahren bedeutet z. B., dass Sie den tatsächlichen Namen einer Datei eingeben müssen. Außerdem werden neue Begriffe sowie die Titel von Dokumentationen in Kursivschrift angegeben.
%SystemRoot%	Das Windows-Systemverzeichnis, das WTSRV, WINNT, WINDOWS oder ein anderer Verzeichnisname sein kann, den Sie bei der Installation von Windows angegeben haben.
`Nichtproportional`	Text, der in einer Textdatei angezeigt wird.
{geschweifte Klammern}	Eine Reihe von Elementen, von denen eines in Befehlsanweisungen erforderlich ist. Beispiel: **{ ja | nein }** bedeutet, dass Sie entweder **ja** oder **nein** eingeben müssen. Geben Sie die Klammern selbst nicht mit ein.
[eckige Klammern]	Optionale Elemente in Befehlsanweisungen. Beispiel: **[/ping]** bedeutet, dass Sie **/ping** zusammen mit dem Befehl eingeben können. Geben Sie die eckigen Klammern selbst nicht mit ein.
| (vertikaler Strich)	Ein Trennzeichen zwischen Elementen in geschweiften oder eckigen Klammern in Befehlsanweisungen. Beispiel: **{ /hold | /release | /delete }** bedeutet, dass Sie **/hold** oder **/release** oder **/delete** eingeben.
… (Auslassung)	Sie können das vorherige Element bzw. die vorherigen Elemente in Befehlsanweisungen wiederholen. Beispiel: **/route:***Gerätename***[,...]** bedeutet, dass Sie weitere *Gerätenamen*, durch Kommas voneinander getrennt, eingeben können.

Weitere Informationen und Support

In diesem Abschnitt wird die Dokumentation zu diesem Release beschrieben. Außerdem wird beschrieben, wie Sie weitere Informationen zu Password Manager erhalten.

Die folgenden Themen werden behandelt:

- Produktdokumentation
- Kundendienst und technischer Support
- Subscription Advantage
- Schulung und Zertifizierung

Produktdokumentation

Weitere Password Manager-Dokumentation finden Sie auf der Citrix Website (http://www.Citrix.com). Direkte Links zur Dokumentation finden Sie in der Datei Password_Manager_Read_Me_First.html im Ordner \Documentation auf der Produkt-CD.

Hinweis: Handbücher werden im PDF-Format bereitgestellt. Zum Anzeigen, Durchsuchen und Drucken von PDF-Dokumenten benötigen Sie Adobe Acrobat Reader 5.0.5 mit Acrobat Search oder Adobe Reader 6.0 oder höher. Diese Produkte stehen zum kostenlosen Download auf der Website von Adobe Systems unter http://www.adobe.com bereit.

---

zur Installation

Die Update-Informationen zur Installation umfassen Informationen zur Installation, die nach Fertigstellung der Readmedatei zusammengestellt wurden. Die Update-Informationen finden Sie unter http://support.citrix.com/article/CTX111284.

Password_Manager_Read_Me_First

Das Dokument Password_Manager_Read_Me_First.html, das auch *Willkommen bei Citrix Password Manager* genannt wird, finden Sie im Order \Documentation auf der Produkt-CD. Das Dokument enthält direkte Links zur Bibliothek der Password Manager-Dokumentation auf der Citrix Website.

Readmedateien

Die Readmedatei enthält Informationen zur Funktionalität von Password Manager, zu bekannten Problemen und Änderungen sowie weitere wichtige Informationen, die nach Fertigstellung des *Citrix Password Manager-Administratorhandbuchs* zusammengestellt wurden. Lesen Sie unbedingt diese Datei, bevor Sie mit der Installation von Password Manager beginnen. Es befindet sich auf der Citrix Website und kann direkt über die Datei Password_Manager_Read_Me_First.html geöffnet werden.

Handbuch „Schnelleinstieg für die Citrix Lizenzierung“

Die Lizenzierung für Password Manager hat sich seit Password Manager 4.1 geändert. Weitere Informationen zum Zuweisen und Erstellen einer Lizenzdatei und dem Download der Datei auf den Lizenzserver finden Sie im Handbuch *Schnelleinstieg für die Citrix Lizenzierung*. Links zu diesem Handbuch finden Sie in der Datei Password_Manager_Read_Me_First.html und im Citrix Knowledge Center auf der Seite „Top Licensing Resources“ unter http://support.citrix.com/licensing/.

Citrix Password Manager-Installationshandbuch

In diesem Handbuch finden Sie Installations- und Upgradeschritte für Password Manager. Es befindet sich auf der Citrix Website und kann direkt über die Datei Password_Manager_Read_Me_First.html geöffnet werden.

Citrix Password Manager-Administratorhandbuch

Im Administratorhandbuch finden Sie konzeptionelle Informationen und Anweisungen für Systemadministratoren, die Komponenten von Password Manager verwalten, konfigurieren und testen. Es befindet sich auf der Citrix Website und kann direkt über die Datei Password_Manager_Read_Me_First.html geöffnet werden.

Installationscheckliste

Dieses Dokument ist eine kurze Anleitung für Administratoren, die mit der Installation von Password Manager vertraut sind. Der Installationsvorgang wird sehr grob beschrieben. Die Installationscheckliste ist kein Ersatz für dieses Installationshandbuch. Es befindet sich auf der Citrix Website und kann direkt über die Datei Password_Manager_Read_Me_First.html geöffnet werden.

Onlinehilfe für Administratoren und Benutzer

Für Administratoren stehen nun in großem Umfang Hilfethemen auf Grundlage des Installations- und Administratorhandbuches bereit. Administratoren können Informationen zu häufigen Aufgaben, Arbeitsabläufen und Einstellungen auf dem Bildschirm anzeigen.

Die Benutzer erhalten Informationen zu häufigen Aufgaben, u. a. zum Erstellen von Anmeldeinformationen für Anwendungen, zum Verwenden des Anmeldungsmanagers und zum Einstellen von automatischen Password Manager-Funktionen. Die Benutzer können die Hilfe über das Menü **Hilfe** oder die Schaltfläche **Hilfe** aufrufen.

Citrix Password Manager Evaluator's Guide

Dieses Handbuch bietet einen Überblick über die Funktionen und die Funktionalität von Password Manager. Es enthält Anweisungen zum Einrichten und Ausführen einer kleinen Testumgebung für die Bereitstellung des Produkts.

Kundendienst und technischer Support

Citrix bietet technischen Support hauptsächlich über Citrix Solutions Advisors an. Wenden Sie sich zuerst an Ihren Vertragshändler oder suchen Sie unter http://www.citrix.com nach dem nächstgelegenen Solution Advisor.

Zusätzlich zu Citrix Solution Advisors bietet Citrix zahlreiche Tools zum online technischen Support und Selbstbedienungssupport im Knowledge Center unter http://support.citrix.com/ an. Das Knowledge Center bietet u. a. Folgendes:

- Eine Knowledge Base mit Tausenden von technischen Lösungen zur Unterstützung der Citrix Umgebung.
- Eine webbasierte Produktdokumentationsbibliothek.
- Interaktive Support-Foren für jedes Citrix Produkt.
- Zugriff auf die neuesten Hotfixes und Service Packs.
- Security Bulletins.
- Webbasierte Problemmeldung und –verfolgung (für Benutzer mit gültigen Supportverträgen).
- Citrix Live Remote Assistance. Mit dem Produkt von Citrix für die Remoteunterstützung, GoToAssist, kann ein Supportmitarbeiter Ihren Desktop sehen und die Maus- und Tastatur zusammen mit Ihnen verwenden, um Ihnen bei der Lösung eines Problems zu helfen.

Eine andere Supportquelle, Citrix Preferred Support Services, bietet eine Reihe von Optionen, sodass Sie den Grad und die Art von Support für die Citrix Produkte in Ihrer Organisation anpassen können.

Subscription Advantage

Subscription Advantage stellt die einfachste und bequemste Möglichkeit dar, Ihre Citrix Software mit den neuesten serverbasierten Funktionen auf dem Laufenden zu halten. Während der Laufzeit des Abonnements erhalten Sie regelmäßig automatisch Folgendes:

- Feature Releases
- Softwareupgrades
- Erweiterungen
- Wartungs-Releases
- Bevorzugten Zugang zu wichtigen technischen Informationen von Citrix

Weitere Informationen zum Abonnement finden Sie auf der Citrix Website unter http://www.citrix.com/services/ (klicken Sie auf **Subscription Advantage**). Weitere Informationen erhalten Sie auch von Ihrem Citrix Vertragshändler oder einem Mitglied von Citrix Solutions Advisors.

Schulung und Zertifizierung

Citrix bietet eine Reihe von unterrichteten (ILT, engl. instructor led training) und webbasierten Kursen (WBT, engl. web-based training). Die von einem Schulungsleiter durchgeführten ILT-Kurse werden von Citrix Authorized Learning Centers (CALCs) angeboten. CALCs bieten hochwertige Schulungen mit den professionellen Schulungsmaterialien von Citrix. Viele diese Kurse bereiten auf eine Zertifizierung vor.

Webbasierte Schulungskurse werden auch von CALCs, Wiederverkäufern und über die Website von Citrix angeboten.

Informationen zu Programmen und Schulungsunterlagen für Citrix Schulungen und Zertifikate finden Sie unter http://www.citrix.com.

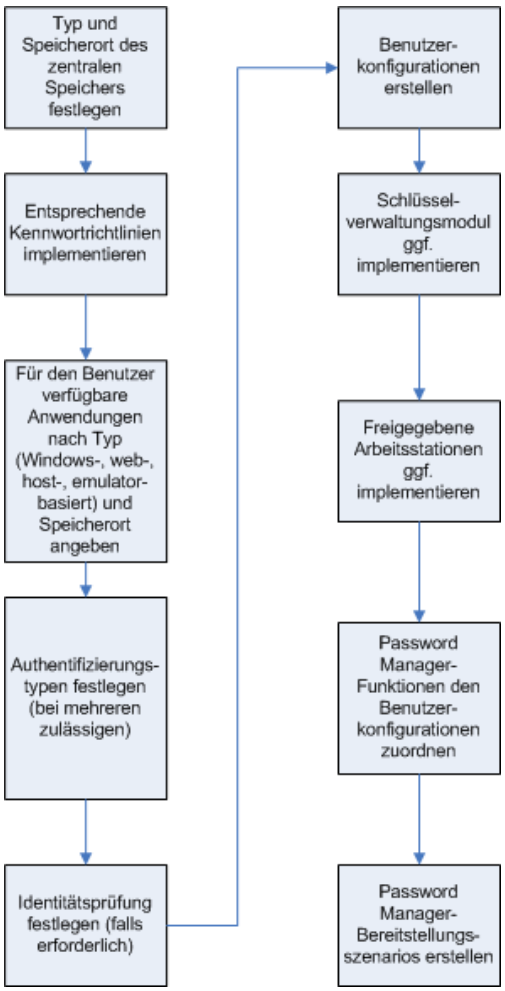
Planen der Password Manager-Umgebung

Dieser Abschnitt enthält Informationen zum Planen der Password Manager-Umgebung und zum Implementieren von Password Manager.

Die folgenden Themen werden behandelt:

- „Diagramm des Planungsablaufs“ auf Seite 20
- „Erste Schritte“ auf Seite 21
- „Auswählen des Typs des zentralen Speichers“ auf Seite 23
- „Verwenden von Kennwortrichtlinien für den Zugriff auf Anwendungen“ auf Seite 33
- „Typen der im Unternehmen verwendeten Single Sign-On-aktivierten Anwendungen“ auf Seite 39
- „Typen der im Unternehmen verwendeten Smartcards“ auf Seite 42
- „Verwenden der Identitätsprüfung“ auf Seite 44
- „Planen der Benutzerkonfigurationen“ auf Seite 48
- „Gemeinsames Verwenden von Ressourcen oder Arbeitsstationen (Hotdesktop)“ auf Seite 51
- „Auswählen optionaler Funktionen des Password Manager-Dienstes“ auf Seite 57
- „Bereitstellungsszenarios für Password Manager Agent“ auf Seite 63
- „Richtlinien für mehrere primäre Authentifizierungsmethoden und Methoden zum Schutz der Anmeldeinformationen der Benutzer“ auf Seite 65

Diagramm des Planungsablaufs


Typ und Speicherort des zentralen Speichers festlegen
Entsprechende Kennwortrichtlinien implementieren
Für den Benutzer verfügbare Anwendungen nach Typ (Windows-, web-, host-, emulator-basiert) und Speicherort angeben
Authentifizierungs-typen festlegen (bei mehreren zulässigen)
Identitätsprüfung festlegen (falls erforderlich)
Benutzer-konfigurationen erstellen
Schlüssel-verwaltungsmodul ggf. implementieren
Freigegebene Arbeitsstationen ggf. implementieren
Password Manager-Funktionen den Benutzer-konfigurationen zuordnen
Password Manager-Bereitstellungs-szenarios erstellen

Erste Schritte

Eine Password Manager-Umgebung kann die folgenden Elemente enthalten:

- Freigegebene Netzwerkordner oder Active Directory mit dem zentralen Speicher.
- Einen oder mehrere Computer, auf denen die Password Manager Console ausgeführt wird.
- PCs der Benutzer, auf denen Password Manager Agent ausgeführt wird.
- Einen dedizierten Server, auf dem der Password Manager-Dienst ausgeführt wird und auf dem ein oder mehrere Module installiert sind.
- Citrix Presentation Server-Umgebung mit Password Manager Agent.
- Authentifizierungsgeräte, z. B. Smartcards.
- Password Manager-Funktionen, z. B. Hotdesktop und Schlüsselverwaltung.

Nachdem Sie einen grundlegenden oder auch vollständigen Plan für Password Manager erstellt haben, können Sie den Plan in der Umgebung implementieren. In der folgenden Tabelle wird beschrieben, welche Schritte für die Erstverwendung von Password Manager erforderlich sind.

Aufgabe	**Siehe Abschnitt**
1. Ermitteln der Funktionen, die Sie in der Umgebung implementieren möchten	• „Planen der Password Manager-Umgebung“ auf Seite 19 (dieser Abschnitt) • „Benutzerauthentifizierung und Identitätsprüfung“ im *Citrix Password Manager-Administratorhandbuch* • „Verwalten der fragenbasierten Authentifizierung“ im *Citrix Password Manager-Administratorhandbuch* • „Benutzerseitiges Verwalten der primären Anmeldeinformationen mit dem Konto-Self-Service“ im *Citrix Password Manager-Administratorhandbuch* • „Automatisieren der Eingabe der Anmeldeinformationen mit dem Provisioning“ im *Citrix Password Manager-Administratorhandbuch* • „Hotdesktop: Desktopfreigabeumgebung für Benutzer“ im *Citrix Password Manager-Administratorhandbuch*

Aufgabe	Siehe Abschnitt
2. Erstellen eines zentralen Speichers und Installieren der Komponenten von Password Manager mit optionalen Funktionen Aktualisieren einer bestehenden Installation von Password Manager	• „Auswählen des Typs des zentralen Speichers“ auf Seite 23 • „Installieren von Password Manager“ auf Seite 75 • „Aktualisieren von Password Manager“ auf Seite 133
3. Erstellen, Bearbeiten oder Überprüfen der Kennwortrichtlinien	• „Verwenden von Kennwortrichtlinien für den Zugriff auf Anwendungen“ auf Seite 33 • „Verwenden von Kennwortrichtlinien zum Erzwingen von Kennwortanforderungen“ im *Citrix Password Manager-Administratorhandbuch*
4. Erstellen oder Bearbeiten der Anwendungsdefinitionen	• „Typen der im Unternehmen verwendeten Single Sign-On-aktivierten Anwendungen“ auf Seite 39 • „Verwenden und Verwalten von Anwendungsdefinitionen“ im *Citrix Password Manager-Administratorhandbuch*
5. Erstellen von Benutzerkonfigurationen auf der Grundlage der Unternehmensanforderungen	• „Planen der Benutzerkonfigurationen“ auf Seite 48 • „Erstellen von Benutzerkonfigurationen“ im *Citrix Password Manager-Administratorhandbuch*
6. Installieren der Agentsoftware auf Benutzerdesktops oder auf Servern mit Presentation Server	• „Bereitstellungsszenarios für Password Manager Agent“ auf Seite 63 • „Installieren und Konfigurieren von Password Manager Agent“ auf Seite 117
7. Informieren der Benutzer über die sichere Speicherung der Amelde-informationen für Anwendungen mit Password Manager	Maßgebliche operative Richtlinien bzw. IT-Handbuch des Unternehmens

Auswählen des Typs des zentralen Speichers

Hinweis: Sie können einen zentralen Speicher als Teil des Installationsvorgangs von Password Manager automatisch erstellen oder mit dem Dienstprogramm zum Setup des zentralen Speichers manuell einrichten. Weitere Informationen finden Sie unter „Erstellen eines zentralen Speichers“ auf Seite 96 und „Erstellen eines zentralen Speichers an einer Befehlszeile (optional)“ auf Seite 99.

Password Manager verwendet ein Repository, den so genannten zentralen Speicher, zum Speichern und Abrufen von Informationen über Benutzer und die Umgebung. Password Manager benötigt die Daten im zentralen Speicher für die Ausführung aller standardmäßigen und konfigurierten Single Sign-On-Funktionen.

Der zentrale Speicher enthält Benutzerdaten und administrative Daten:

- **Benutzerdaten** im zentralen Speicher sind u. a. die sekundären Anmeldeinformationen des Benutzers, Sicherheitsfragen und Antworten, dienstspezifische Daten (z. B. Provisioningdaten, fragenbasierte Authentifizierungsdaten, Registrierung für die Schlüsselwiederherstellung usw.) sowie die Password Manager zugeordneten Benutzerdaten der Windows-Registrierung.
- **Administrative Daten** im zentralen Speicher sind u. a. Anwendungsdefinitionen, Kennwortrichtlinien, Sicherheitsfragen und weitere Einstellungen, die in der Konsole für Funktionen und Komponenten von Password Manager festgelegt werden.

Im Wesentlichen ermöglicht der zentrale Speicher die Kommunikation der auf einem PC des Benutzers oder unter Citrix Presentation Server ausgeführten Agentsoftware mit dem zentralen Speicher und den Diensten, um Anmeldeinformationen des Benutzers an Anwendungen bereitzustellen, auf die der Benutzer zugreifen darf.

Der Agent verwaltet einen lokalen Speicher auf dem PC des Benutzers. Im lokalen Speicher werden lediglich die sekundären Anmeldeinformationen des Benutzers, die Informationen zur Schlüsselwiederherstellung und ggf. die Sicherheitsfragen und Antworten gespeichert. Der Agent ist mit dem zentralen Speicher synchronisiert. So können sich die Benutzer frei im Unternehmen bewegen und haben jederzeit Zugriff auf die gespeicherten Anmeldeinformationen.

Typen des zentralen Speichers sind:

- Active Directory

  Der zentrale Speicher verwendet die Active Directory-Umgebung und -Objekte zum Speichern und Aktualisieren von Password Manager-Daten.

  Weitere Informationen finden Sie unter „Auswählen von Active Directory als zentralen Speicher“ auf Seite 25.

- NTFS-Netzwerkfreigabe

  Der zentrale Speicher verwendet eine Windows-Netzwerkfreigabe zum Speichern von Password Manager-Daten. Weitere Informationen finden Sie unter „Auswählen einer NTFS-Netzwerkfreigabe“ auf Seite 27.

- Freigegebener Novell Ordner

  Der zentrale Speicher verwendet einen freigegebenen Ordner von Novell NetWare zum Speichern von Password Manager-Daten.

  Weitere Informationen finden Sie unter „Auswählen eines freigegebenen Novell Ordners“ auf Seite 29.

Hinweis: Mit Citrix Password Manager können Sie Benutzer von einem Typ des zentralen Speichers auf einen anderen migrieren, falls Sie zu einem späteren Zeitpunkt feststellen, dass ein bestimmter Speichertyp besser geeignet ist als der aktuell in der Umgebung verwendete. Weitere Informationen finden Sie unter „Verschieben von Daten in einen anderen zentralen Speicher“ im *Citrix Password Manager-Administratorhandbuch*

Hinweis: Weitere Informationen zu Enterprise-Gesamtstrukturen mit mehreren Domänen finden Sie unter „Verwenden der Kontozuordnung mit mehreren zentralen Speichern und Kontoanmeldeinformationen der Benutzer in einem Unternehmen mit mehreren Domänen“ auf Seite 30.

Weitere Informationen zu den Benutzerkonfigurationen in Umgebungen mit mehreren Domänencontrollern finden Sie auch unter „Angeben der Domänencontroller für Benutzerkonfigurationen“ im *Citrix Password Manager-Administratorhandbuch*.

Auswählen von Active Directory als zentralen Speicher

Wenn Sie Active Directory als zentralen Speicher auswählen, können Sie die Vorteile der bestehenden Active Directory-Benutzerauthentifizierung und -Objektverwaltung nutzen. Sie können z. B. benutzerspezifische Einstellungen auf jede Domänenstufe (Domäne, Organisationseinheit, Gruppe oder Benutzer) anwenden.

Wenn Sie den zentralen Speicher in Active Directory erstellen, werden dem Active Directory-Schema zwei neue Klassen und zwei Attribute hinzugefügt:

Klasse	Beschreibung
citrix-SSOConfig	Beschreibt das Objekt, das die Daten für die Agenteinstellungen enthält, den Synchronisierungsstatus, die Anwendungs-definitionen sowie für die Festlegung des Agentverhaltens). Diese Klasse umfasst die folgenden Attribute: citrix-SSOConfigData: Enthält die eigentlichen Daten citrix-SSOConfigType: Gibt den Datentyp an
citrix-SSOSecret	Beschreibt das geheime Datenobjekt, das für die Authentifizierung eines Benutzers von Password Manager verwendet wird. Diese Klasse enthält das folgende Attribut: citrix-SSOSecretData: Enthält verschlüsselte Anmelde-informationsdaten für Anwendungen sowie Daten für das benutzerseitige Zurücksetzen des Kennworts

Hinweis: Weitere Informationen zu diesen Klassen und Attributen finden Sie auf der Produkt-CD von Password Manager in der Datei CitrixMPMSchema.xml im Ordner \Tools.

Wählen Sie Active Directory als zentralen Speicher aus, wenn Folgendes zutrifft:

- Sie können das Active Directory-Schema ohne Auswirkungen auf das Unternehmen erfolgreich erweitern.
- Sie haben bereits das von Microsoft empfohlene Active Directory-Backup und die Active Directory-Wiederherstellung implementiert (obwohl dies keine Voraussetzung ist).
- Sie möchten die in Active Directory integrierte hohe Verfügbarkeit auf die Daten des zentralen Speichers ausdehnen.

Vorteile

- Active Directory bietet integriertes Failover und integrierte Redundanz. Zusätzliche Maßnahmen für die Wiederherstellung im Notfall sind nicht erforderlich.
- Mit der Active Directory-Replikation können Sie die im zentralen Speicher enthaltenen administrativen Daten und Benutzerdaten im Unternehmen verteilen.
- Beim Verwenden von Active Directory als zentralen Speicher ist keine weitere Hardware erforderlich.

Überlegungen

- Die Verwendung von Active Directory als zentralen Speicher erfordert die Erweiterung des Schemas und damit eine sorgfältige Planung und Implementierung. Das Erweitern des Schemas wirkt sich auf die komplette Gesamtstruktur aus.
- Es empfiehlt sich, die Erweiterung des Schemas und Erstellung des zentralen Active Directory-Speichers außerhalb der Spitzenauslastungszeiten vorzunehmen. Die Active Directory-Replikationszykluslatenz hat Auswirkungen auf die Geschwindigkeit, mit der die Änderungen auf alle Domänencontroller in der Gesamtstruktur kopiert werden.
- Für die standortübergreifende Replikation von Daten des zentralen Speichers in großen Unternehmen mit WANs muss die Replikation richtig konfiguriert werden, um die Latenz zur verringern. (Die Replikation innerhalb eines Standorts dagegen führt normalerweise zu einer geringeren Latenz.)

Auswählen einer NTFS-Netzwerkfreigabe

Wichtig: Citrix empfiehlt in diesem Fall die Verwendung einer versteckten Freigabe für den zentralen Speicher. Wenn Sie einen zentralen Speicher wie unter „Erstellen eines zentralen Speichers“ auf Seite 96 oder „Erstellen eines zentralen Speichers an einer Befehlszeile (optional)“ auf Seite 99 beschrieben erstellen, wird automatisch eine versteckte Freigabe erstellt.

Wenn Sie eine NTFS-Netzwerkfreigabe als zentralen Speicher verwenden, können Sie die Vorteile der bestehenden Active Directory-Benutzerauthentifizierung und -Struktur nutzen, ohne das Active Directory-Schema erweitern zu müssen. Sie können z. B. benutzerspezifische Einstellungen auf jede Domänenstufe (Domäne, Organisationseinheit, Gruppe oder Benutzer) anwenden.

Password Manager erstellt einen freigegebenen Ordner mit dem Namen CITRIXSYNC sowie die beiden Unterordner People und CentralStoreRoot.

Der Ordner People enthält für jeden Benutzer einen Unterordner mit den entsprechenden Lese- und Schreibberechtigungen. Der Ordner CentralStoreRoot enthält administrative Daten.

Vorteile

- Sie können die Darstellungsweise eines zentralen Active Directory-Speichers emulieren, ohne das Active Directory-Schema erweitern zu müssen. Sie können jedoch die Vorteile der bestehenden Active Directory-Hierarchie oder -Gruppen nutzen.

  Hinweis: Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.

- Die Benutzerdaten sind immer aktuell, da sie an einem zentralen Speicherort aufbewahrt werden und die mit Active Directory einhergehende Latenz bei der Datenreplikation vermieden wird.
- Um eine höhere Verfügbarkeit zu gewährleisten, können Sie einen Lastausgleich der Freigaben auf mehreren Computern ausführen, die NTFS-Netzwerkfreigaben hosten können.
- Die Arbeitslast im Zusammenhang mit den Authentifizierungsaufgaben in der Active Directory-Umgebung wird reduziert.
- Wenn Sie zu einem späteren Zeitpunkt Active Directory als zentralen Speicher implementieren möchten, können Sie mit Password Manager den als zentralen Speicher verwendeten freigegebenen NTFS-Ordner auf Active Directory migrieren.

Überlegungen

- Unter Umständen wird zusätzliche Hardware zum Hosten des zentralen Speichers benötigt.
- Die Dateien und Ordner des zentralen Speichers (einschließlich der dazugehörigen Berechtigungen) müssen regelmäßig gesichert werden. Sie sollten auch Wiederherstellungspläne für den Notfall bereithalten und implementieren, wenn Sie die Replikation von Dateien und Ordnern für die Wiederherstellung von Sites benötigen.
- Die Netzwerktopologie des Unternehmens macht es u. U. für Benutzer (und Password Manager Agent) erforderlich, Benutzerdaten über eine oder mehrere WAN-Verbindungen hinweg zu transferieren. In diesem Fall sollten Sie die im Lieferumfang von Microsoft Windows 2000 Server oder Server 2003 enthaltene DSF-Technologie (verteiltes Dateisystem) implementieren. Weitere Informationen zu dieser Technologie finden Sie auf der Microsoft Website unter http://support.microsoft.com.

Auswählen eines freigegebenen Novell Ordners

Wichtig: Password Manager-Dienste werden in Password Manager-Umgebungen mit freigegebenen Novell Ordnern nicht unterstützt.

Wenn Sie einen freigegebenen Novell NetWare-Ordner als zentralen Speicher verwenden, können Sie die Vorteile der bestehenden Novell NetWare Directory Services (NDS) nutzen. Die Verwendung dieses Typs des zentralen Speichers ähnelt der einer NTFS-Netzwerkfreigabe.

Richten Sie einen sicheren Netzwerkordner in eDirectory ein und speichern Sie darin alle der Password Manager-Umgebung zugeordneten Daten. Anwendungen und Einstellungen können auf der Domänenstufe definiert und zugeordnet werden.

Vorteile

- Sie implementieren bereits Novell NetWare Directory Services.
- Als zentraler Speicher kann ein bestehender und sicherer freigegebener Ordner verwendet werden.

Überlegungen

- Die Zuordnung von Benutzerkonfigurationen zu Active Directory-Gruppen wird von diesem Typ des zentralen Speichers nicht unterstützt.
- Bei Verwendung eines freigegebenen Novell NetWare-Ordners muss das Novell Kennwort der Benutzer mit dem Windows-Kennwort übereinstimmen. Diese Anforderung gilt für Umgebungen, in denen Novell ZENworks for Desktops mit Unterstützung für Windows Dynamic Local User (DLU) auf dem NDS-Server und Novell Workstation Manager auf jedem Computer mit der Password Manager Agent-Software ausgeführt werden.

- Da die Agentsoftware ein Windows-Kennwort verwendet, müssen bei der Verwendung der Novell Netware-Datensynchronisierung die Kennwörter der Benutzer für Novell und Windows identisch sein.
- Der zentrale Speicher muss in derselben Struktur sein wie die Computer, auf denen Instanzen der Agentsoftware installiert sind. Benutzer müssen sich an einer Novell-Struktur anmelden, die den freigegebenen Ordner enthält. Darüber hinaus benötigen die Benutzer auch Konten mit Leseberechtigung für den freigegebenen Ordner von Novell Netware, den Sie als zentralen Speicher angegeben haben.
- Password Manager-Dienste werden in Password Manager-Umgebungen mit freigegebenen Novell Ordnern nicht unterstützt.

Verwenden der Kontozuordnung mit mehreren zentralen Speichern und Kontoanmeldeinformationen der Benutzer in einem Unternehmen mit mehreren Domänen

Hinweis: Weitere Informationen zur Konfiguration der Kontozuordnung finden Sie unter „Synchronisieren von Anmeldeinformationen mit der Kontozuordnung“ im *Citrix Password Manager-Administratorhandbuch*.

Administratoren können in Unternehmen mit mehreren Domänen mehrere zentrale Speicher einrichten. In einer solchen Umgebung ist es sogar möglich, mehrere Typen des zentralen Speichers zu verwenden. So können Sie z. B. Benutzerkonfigurationen in einer Domäne dem Speichertyp NTFS-Netzwerkfreigabe zuweisen und in einer anderen Domäne dem Speichertyp Active Directory.

Unternehmen haben möglicherweise mehrere Windows-Domänen, und Benutzer können daher mehrere Windows-Konten haben. Mit der Kontozuordnungsfunktion in Password Manager kann sich ein Agentbenutzer von einem oder mehreren Windows-Konten aus an jeder Anwendung anmelden. Da Password Manager normalerweise Anmeldeinformationen des Benutzers mit einem Konto verbindet, werden die Anmeldeinformationen nicht automatisch zwischen mehreren Konten des Benutzers synchronisiert.

Administratoren können jedoch die Kontozuordnung konfigurieren und die Anmeldeinformationen des Benutzers mit dem Modul **Synchronisierung der Anmeldeinformationen** synchronisieren. Benutzer, für die die Kontozuordnung konfiguriert ist, können mit jedem ihrer Konten in der Password Manager-Umgebung auf alle Anwendungen zugreifen. Wenn die Anmeldeinformationen des Benutzers geändert, hinzugefügt oder von einem Konto entfernt werden, werden die Anmeldeinformationen automatisch mit jedem zugeordneten Konto des Benutzers synchronisiert.

Ohne die Kontozuordnung muss ein Benutzer, der mehrere Windows-Konten besitzt, die Anmeldeinformationen manuell für jedes Windows-Konto ändern.

Vorteile

- Die Kontozuordnung steigert die Produktivität und verringert die Inanspruchnahme des Helpdesks, da die Anmeldeinformationen des Benutzers synchronisiert werden und damit das Verwalten oder das Fehlschlagen der Anmeldungen verringert wird.
- Konten können über verschiedene Typen des zentralen Speichers synchronisiert werden. Das heißt, das ein Benutzerkonto, das Active Directory als zentralen Speicher verwendet, mit einem zugeordneten Konto synchronisiert werden kann, das als zentralen Speicher eine NTFS-Netzwerkfreigabe verwendet.
- Konten können auch über verschiedene Benutzerkonfigurations-zuordnungen synchronisiert werden. Sie können z. B. eine Benutzer-konfiguration in einer Domäne einer Active Directory-Hierarchie (OU oder Benutzer) und in einer anderen Domäne einer Active Directory-Gruppe zuordnen.
- Konten können über verschiedene Benutzerkonfigurationszuordnungen in derselben Domäne und demselben zentralen Speicher synchronisiert werden.
- Für die Kontozuordnung müssen keine vertrauenswürdigen Beziehungen zwischen Domänencontrollern bestehen.

Überlegungen

Vor der Konfiguration der Kontozuordnung sollten Sie Folgendes berücksichtigen:

- Die Kontozuordnung ist nicht mit Smartcards kompatibel, wenn Smartcards als primäre Authentifizierungsmethode für die Anmeldung an Windows verwendet werden.

  Hinweis: Die Benutzerkonfigurationen in jeder Domäne haben möglicherweise unterschiedliche Kennwortrichtlinien, wodurch der Zugriff auf eine Ressource blockiert werden könnte. Mit der Kontozuordnungsfunktion werden jedoch nur die Anmeldeinformationen der Benutzer synchronisiert, nicht die Konfigurationsrichtlinien. Überlegen Sie sich, wie Sie Kennwortrichtlinien im Unternehmen abfassen.

- Jedes zugeordnete Domänenkonto muss Citrix Password Manager verwenden.
- Anwendungsdefinitionsnamen müssen in jeder Benutzerkonfiguration identisch sein, damit die Anmeldeinformationen von der Kontozuordnungsfunktion synchronisiert werden können.
- Anmeldeinformationen der Benutzer werden nur für Anwendungen gemeinsam verwendet, die in Anwendungsdefinitionen angegeben sind, die vom Password Manager-Administrator erstellt wurden.
- Als Teil des Password Manager-Dienstes ist das Modul **Synchronisierung der Anmeldeinformationen** ein Webdienst, der über eine sichere HTTP-Verbindung verfügbar ist. Alle Computer im Unternehmen, die die Kontozuordnung verwenden, müssen auf dieses Modul zugreifen können.

Verwenden von Kennwortrichtlinien für den Zugriff auf Anwendungen

Kennwortrichtlinien sind Regeln, mit denen festgelegt wird, wie Kennwörter erstellt, gesendet und verwaltet werden. Die Password Manager-Installation enthält zwei Standardkennwortrichtlinien mit der Bezeichnung *Standardrichtlinie* und *Domänenrichtlinie*. Beide Richtlinien können nicht gelöscht werden.

Sie können die Richtlinien jedoch kopieren und ändern, um sie den im Unternehmen geltenden Richtlinien und Vorschriften anzupassen.

Unter „Standardeinstellungen für die Standardrichtlinie und die Domänenrichtlinie“ auf Seite 36 finden Sie eine Liste der installierten Standardeinstellungen für die Kennwortrichtlinien **Standardrichtlinie** und **Domänenrichtlinie**. Nutzen Sie die Informationen in dieser Tabelle, um die Richtlinien zu ändern oder eigene Richtlinien zu erstellen.

Standardkennwortrichtlinie

Password Manager wendet die **Standardrichtlinie** auf alle kennwortaktivierten Anwendungen im Unternehmen an (außer auf Anwendungen, für die die Angabe von Domänenanmeldeinformationen des Benutzers erforderlich ist; weitere Informationen finden Sie unter „Domänenkennwortrichtlinie“ auf Seite 34). Die Richtlinie wird auf alle Anwendungen angewendet, die nicht von einem Administrator (mit der Anwendungsdefinitionsfunktion in der Konsole) definiert wurden, bzw. auf alle Anwendungen, die nicht Teil einer Anwendungsgruppe sind.

Wenn ein Benutzer im Anmeldungsmanager der Agentsoftware Anmeldeinformationen für eine Anwendung hinzufügt, die keine entsprechende Anwendungsdefinition hat, verwendet Password Manager die Standardrichtlinie zur Verwaltung dieser Anwendung.

Domänenkennwortrichtlinie

Normalerweise erstellt ein Administrator eine Anwendungsgruppe und weist dann den Anwendungen in dieser Gruppe die Domänenrichtlinie zu. Password Manager weist daraufhin denjenigen Anwendungen die Domänenrichtlinie zu, welche die Domänenanmeldeinformationen des Benutzers für den Zugriff benötigen. Sie können die Domänenrichtlinie ändern oder kopieren, sodass sie die für Active Directory bzw. NT geltenden Domänenrichtlinien für Benutzerkonten im Unternehmen widerspiegeln.

Wenn Sie eine Anwendungsgruppe als Domänenkennwortgruppe behandeln möchten, müssen Sie die Domänenrichtlinie auf diese Anwendungsgruppe anwenden.

Hinweis: Eine Anwendungsgruppe ist eine Sammlung von definierten Anwendungen mit mindestens einer dazugehörigen Benutzerkonfiguration, einschließlich der Richtlinie für die Verwaltung der Anwendungen.

Benutzerdefinierte Kennwortrichtlinien

Wichtig: Achten Sie beim Erstellen oder Ändern von benutzerdefinierten Kennwortrichtlinien darauf, dass diese zu den Unternehmens- und Anwendungsanforderungen passen. Wenn Sie z. B. eine Richtlinie erstellen, die absolut nicht mit den Anforderungen einer Anwendung übereinstimmt, können sich die Benutzer möglicherweise nicht an dieser Anwendung authentifizieren.

Kennwortrichtlinien können nach Bedarf erstellt werden: Sie können eine Richtlinie auf die gesamte Domänengruppe anwenden, einzelne Richtlinien erstellen und diese zum besseren Schutz der Anwendungen auf einzelne Anwendungsgruppen anwenden usw.

Mit Kennwortrichtlinien legen Sie im Wesentlichen die folgenden Einschränkungen fest:

- Mindest- und Höchstanzahl der Zeichen im Kennwort
- Verwendung von Buchstaben und Ziffern
- Höchstanzahl wiederholter Zeichen
- Nicht erlaubte bzw. benötigte Zeichen oder Sonderzeichen
- Benutzerseitiges Anzeigen der gespeicherten Kennwörter
- Anzahl der Anmeldeversuche
- Parameter für den Ablauf der Kennwörter
- Kennwortverlauf und Ausnahmen

Überlegungen

- Denken Sie bei den Überlegungen zu den Sicherheitsanforderungen immer auch an die Benutzerfreundlichkeit. Zu restriktive Kennwörter können von den Benutzern möglicherweise zu schwer erstellt, implementiert oder behalten werden.
- Da Password Manager inhärent sicher ist, definiert die Standardrichtlinie das Mindestmaß an Kennwortsicherheit, das von Citrix Systems, Inc. zur Sicherung der meisten Anwendungen mit aktiviertem Single Sign-On empfohlen wird. Diese Einstellungen können Sie gemäß den im Unternehmen geltenden Richtlinien und Vorschriften ändern.
- Da Password Manager die Standardrichtlinie auf vom Benutzer hinzugefügte Anwendungen anwendet, sollte die Standardrichtlinie so weit wie möglich gefasst werden, damit Kennwörter für Anwendungen angenommen werden können, für die die Benutzer Kennwörter speichern dürfen.
- Für den Fall eines Kennwortwechsels durch den Benutzer kann die Benutzerkonfiguration in Password Manager so eingestellt werden, dass Password Manager das alte Kennwort mit dem neuen vergleicht. Dies verhindert, dass Benutzer identische Kennwörter für dieselbe Anwendung zweimal hintereinander verwenden.
- Manchmal haben Benutzer ein Kennwort, das für mehrere Anwendungen verwendet wird (z. B. bei einer Produktsuite). Dies wird als gemeinsame Kennwortverwendung bezeichnet. Dabei wird dieselbe Authentifizierungsstelle für die Anwendungen verwendet.

Die anderen Anmeldeinformationen für diese Anwendungen (z. B. Benutzername und benutzerdefinierte Felder) können unterschiedlich sein, das Kennwort des Benutzers ist jedoch gleich. Erstellen Sie in diesem Fall eine Anwendungsgruppe, die eine Kennwortgruppe ist. So stellen Sie sicher, dass die Agentsoftware das Kennwort für alle Anwendungen in der Gruppe als Einheit verwaltet. Bei der Änderung des Kennworts in einer Anwendung stellt die Agentsoftware sicher, dass die Kennwortänderung in den gespeicherten Anmeldeinformationen aller Anwendungen in der Gruppe widergespiegelt wird.

- Domänenkennwortgruppen unterscheiden sich von anderen Kennwortgruppen, da das Domänenkennwort des Benutzers als Hauptkennwort für die Anwendungsgruppe verwendet wird. Wenn der Benutzer das Domänenkennwort ändert, stellt die Agentsoftware sicher, dass die Änderung in den Anmeldeinformationen für alle anderen Anwendungen in der Gruppe widergespiegelt wird. Es kann nur das Domänenkennwort geändert werden. Benutzer können nur dann Kennwortänderungen für eine der anderen Anwendungen in der Gruppe vornehmen, wenn der Administrator die Anwendung aus der Domänenkennwortgruppe entfernt.

Standardeinstellungen für die Standardrichtlinie und die Domänenrichtlinie

In der folgenden Tabelle werden die Standardeinstellungen für die Standardkennwortrichtlinie und die Domänenkennwortrichtlinie beschrieben.

Optionen für die Standardrichtlinie und die Domänenrichtlinie	Standardeinstellung	Benutzerdefinierte Einstellung
Agentassistent für Kennwörter	Benutzer wird zur Aktion aufgefordert	
Regeln für Buchstaben		
Groß-/Kleinschreibung der Buchstaben	Groß- und Kleinbuchstaben zulassen	
Mindestanzahl der Kleinbuchstaben	0	
Mindestanzahl der Großbuchstaben	0	
Erstes Zeichen im Kennwort kann Kleinbuchstabe sein	Ja	
Erstes Zeichen im Kennwort kann Großbuchstabe sein	Ja	
Letztes Zeichen im Kennwort kann Kleinbuchstabe sein	Ja	
Letztes Zeichen im Kennwort kann Großbuchstabe sein	Ja	

Optionen für die Standardrichtlinie und die Domänenrichtlinie	Standardeinstellung	Benutzerdefinierte Einstellung
Grundlegende Kennwortregeln		
Höchstanzahl wiederholter Zeichen	6	
Höchstanzahl aufeinanderfolgender gleicher Zeichen	4	
Höchstlänge für Kennwort	20	
Mindestlänge für Kennwort	8	
Ausschlussregeln		
Anwendungsbenutzername im Kennwort nicht zulassen.	Nein	
Teile des Anwendungsbenutzernamens im Kennwort nicht zulassen.	Nein	
Teile des Windows-Benutzernamens im Kennwort nicht zulassen.	Nein	
Windows-Benutzername im Kennwort nicht zulassen.	Nein	
Folgende Liste der Zeichen oder Zeichengruppen von Kennwörtern ausschließen	Optionale Einstellung	
Zeichenanzahl in den Zeichengruppen, die vom Anwendungsbenutzernamen verwendet werden können	0	
Zeichenanzahl in den Zeichengruppen, die vom Windows-Benutzernamen verwendet werden können	0	
Anmeldeeinstellungen		
Benutzer können Kennwort für Anwendungen anzeigen	Nein	
Neuauthentifizierung der Benutzer vor dem Senden der Anwendungsanmeldeinfo erzwingen	Nein	
Anzahl der Anmeldewiederholungs-versuche	1	
Zeitlimit für Wiederholungsversuche	30 Sekunden	
Regeln für Ziffern		
Ziffern im Kennwort zulassen	Ja	
Höchstanzahl der Ziffern	20	
Mindestanzahl der Ziffern	0	

Optionen für die Standardrichtlinie und die Domänenrichtlinie	Standardeinstellung	Benutzerdefinierte Einstellung
Erstes Zeichen im Kennwort kann Ziffer sein	Ja	
Letztes Zeichen im Kennwort kann Ziffer sein	Ja	
Assistent für Kennwortänderungen		
Benutzer können ein systemgeneriertes Kennwort auswählen oder ein eigenes erstellen	Ja	
Kennwort erstellen und ohne Anzeigen des Assistenten an die Anwendung senden	Nein	
Benutzer können nur ein systemgeneriertes Kennwort auswählen	Nein	
Benutzer können nur ein eigenes Kennwort erstellen	Nein	
Kennwortverlauf und -ablauf		
Neues Kennwort darf nicht mit dem alten Kennwort identisch sein	Nein	
Anzahl der Tage für Hinweis der Benutzer auf Kennwortablauf	14	
Anzahl der Tage bis zum Ablauf des Kennworts	42	
Anzahl der gespeicherten alten Kennwörter	1	
Den Anwendungsdefinitionen zugeordnete Einstellungen für Kennwortablauf verwenden	Nein	
Regeln für Sonderzeichen		
Sonderzeichen im Kennwort zulassen	Nein	
Liste zugelassener Sonderzeichen	!@#$^&*( )_+= [ ] \ | ,?	
Höchstanzahl der Sonderzeichen	20	
Mindestanzahl der Sonderzeichen	0	
Erstes Zeichen im Kennwort kann Sonderzeichen sein	Ja	
Letztes Zeichen im Kennwort kann Sonderzeichen sein	Ja	

Typen der im Unternehmen verwendeten Single Sign-On-aktivierten Anwendungen

Hinweis: Password Manager unterstützt die 64-Bit-Version von Internet Explorer. Die 64-Bit-Terminalemulatorsoftware wird nicht unterstützt.

Als Administrator von Password Manager können Sie für jede Anwendung, die Password Manager für die Benutzer verwalten soll, eine Anwendungsdefinition erstellen bzw. eine Anwendungsdefinitionsvorlage ändern. Sie können Anwendungsdefinitionen mit der Konsole oder mit dem eigenständigen Anwendungsdefinitionstool erstellen, das auf Arbeitsstationen ohne Konsole installiert werden kann.

Sie können auch zulassen, dass Benutzer Password Manager die ermittelten Anmeldeinformationen für alle clientseitigen Anwendungen anhand der Einstellungen in den Benutzerkonfigurationen hinzufügen können. Weitere Informationen finden Sie unter “Erstellen von Benutzerkonfigurationen: Assistent für Benutzerkonfigurationen” und „Agentverhalten konfigurieren“ im *Citrix Password Manager-Administratorhandbuch*.

Die Agentsoftware kann bei den meisten Anwendungen Anmeldeänderungen erkennen und darauf reagieren, darunter bei den folgenden Anwendungstypen:

Anwendungstypen	Beschreibung
Windows	32-Bit-Windows-Anwendungen (einschließlich Java-Anwendungen), z. B. Microsoft Outlook, Lotus Notes, SAP oder jede andere kennwortaktivierte Windows-Anwendung
Web	Webanwendungen (einschließlich Java-Applets und SAP), auf die über Microsoft Internet Explorer zugegriffen wird
Host/Mainframe	Hostbasierte Anwendungen, auf die mit einem HLLAPI-kompatiblen Terminalemulator zugegriffen wird

Die Agentsoftware reagiert entsprechend der Anwendungsdefinitionen, die Sie selbst erstellen oder von bestehenden Anwendungsdefinitionsvorlagen kopieren. Anwendungsdefinitionen haben die folgenden Funktionen:

- Sie ermöglichen der Agentsoftware, Anwendungen und die von den Anwendungen für die Verarbeitung der Anmeldeinformationen des Benutzers verwendeten Formulare zu erkennen und darauf zu reagieren.
- Sie enthalten eine Reihe von Kennungen zum Festlegen von Parametern, mit denen die Agentsoftware Anwendungen erkennt und darauf reagiert.

In jeder Definition erstellen Sie Anmeldeformulare und mit Kennwörtern verbundene Formulare, die erforderlich sind, um den Zugriff auf die Anwendung zu aktivieren. Wenn Sie eine Anwendung öffnen, helfen Ihnen die Assistenten für Anwendungsdefinitionen beim Erstellen der Definition. Über die Fensterzuordnungsfunktion von Password Manager erkennen die Assistenten die Formulare und Felder der meisten Anwendungen.

Hinweis: Password Manager bietet Standardanwendungsdefinitionsvorlagen für verschiedene Anwendungen bzw. Anwendungsfunktionen von Citrix. Wenn Sie diese Anwendungsdefinitionsvorlagen anzeigen möchten, klicken Sie in der Konsolenstruktur auf **Anwendungsdefinitionen** und anschließend im Bereich **Häufige Tasks** auf **Vorlagen verwalten**. (Diese Funktionen sind auch im Anwendungsdefinitionstool verfügbar.) Weitere Vorlagen stehen auf der Citrix Support Website unter http://www.citrix.com/passwordmanager/gettingstarted zur Verfügung.

Benötigte Informationen zu den Anwendungen

Stellen Sie vor dem Erstellen einer Anwendungsdefinition die unten aufgeführten Informationen für alle Anwendungen im Unternehmen zusammen, für die Single Sign-On aktiviert ist. Sie können auch eine Anwendung starten, damit der Assistent für Anwendungsdefinitionen bzw. das Anwendungsdefinitionstool einen Teil dieser Informationen für Sie ermittelt.

- Name der ausführbaren Datei der Anwendung und ggf. der Pfad.

  Durch die Angabe des Pfades für eine Anwendung wird die Sicherheit erhöht und sichergestellt, dass die Benutzer tatsächlich die für das Unternehmen qualifizierte Anwendung ausführen.

- Die für alle Anwendungen erforderlichen Felder für die Anmeldeinformationen des Benutzers, z. B. Benutzername, Kennwort und sonstige Felder (Domänenname, sekundäres Kennwort u. a.).

- Sonstige mit Anmeldeinformationen zusammenhängende Felder im Formular, darunter die folgenden Felder für das Ändern des Kennwortes: Anmeldung, Kennwort ändern, Formular für eine erfolgreiche Kennwortänderung (optional), Formular für eine fehlgeschlagene Kennwortänderung (optional).
- Anforderungen an Anwendungen mit gemeinsamer Kennwortverwendung.

  Sie müssen wissen, welche Anwendungen dieselben Authentifizierungsstellen verwenden und somit möglicherweise Teil einer Kennwortgruppe sind. Kennwortgruppen ermöglichen es der Agentsoftware, mehrere Anmeldeinformationen für Anwendungen zu verwalten, die dieselbe Authentifizierungsmethode verwenden. Sie können dieselbe Kennwortrichtlinie auch auf Anwendungsgruppen anwenden. Weitere Informationen finden Sie unter „Erstellen einer Benutzerkonfiguration mit dem Assistenten für Benutzerkonfigurationen“ im *Citrix Password Manager-Administratorhandbuch* .
- Informationen im Zusammenhang mit Terminalemulationsanwendungen.

  Sie müssen z. B. die Kurznamen der Terminalemulatorsitzungen kennen, die für mit HLLAPI (High-Level Language Application Programming Interface) kompatible Terminalemulatoren erforderlich sind.

Typen der im Unternehmen verwendeten Smartcards

Berücksichtigen Sie den im Unternehmen verwendeten Typ der Authentifizierung.

Sobald Sie den Authentifizierungstyp ermittelt und eine entsprechende Datenschutzmethode in der Benutzerkonfiguration gewählt haben, können Sie die Identitätsprüfung von Benutzern implementieren und so die Anmeldeinformationen noch weiter sichern. Weitere Informationen finden Sie unter „Verwenden der Identitätsprüfung“ auf Seite 44. Informationen zu Datenschutzmethoden in einer Unternehmensumgebung, in der mehrere primäre Authentifizierungsmethoden zugelassen sind, finden Sie unter „Richtlinien für mehrere primäre Authentifizierungsmethoden und Methoden zum Schutz der Anmeldeinformationen der Benutzer“ auf Seite 65.

Smartcard-Unterstützung

Citrix hat Smartcards getestet, die der ISO-Norm 7816 (International Organization for Standardization) entsprechen. Diese Karten haben elektrische Kontakte (werden auch als *Kontaktkarten* bezeichnet), die über einen Smartcard-leser eine Schnittstelle zum Computersystem herstellen. Das Lesegerät kann über einen seriellen, einen USB- oder einen PC-Karten-Port (PCMCIA) am Computer angeschlossen sein.

Citrix unterstützt die Verwendung von PC/SC-basierten kryptographischen Smartcards. Diese Karten bieten eine Unterstützung für kryptographische Funktionen, wie beispielsweise digitale Signaturen und Verschlüsselung. Kryptographische Karten eignen sich für die sichere Speicherung privater Schlüssel, wie etwa in PKI-Sicherheitssystemen (Public Key Infrastructure).

Die eigentlichen kryptographischen Vorgänge finden auf der Smartcard selbst statt, sodass der private Schlüssel nie die Karte verlässt. Außerdem stellen Smart-cards eine Zweifaktor-Authentifizierung bereit, mit der die Sicherheit erhöht wird: die Karte und die PIN-Nummer des Benutzers. Wenn diese Elemente zusammen verwendet werden, beweisen sie, dass der Karteninhaber der rechtmäßige Eigentümer der Smartcard ist.

Softwareanforderungen für Smartcards

Welche Voraussetzungen im Hinblick auf die Konfiguration für Ihre spezielle Smartcard-Implementierung zu erfüllen sind, erfahren Sie im Smartcard-Fachhandel. Auf dem Server oder Client werden folgende Komponenten benötigt:

- PC/SC-Software
- CSP-Software (Cryptographic Service Provider)
- Softwaretreiber für den Smartcardleser

Unter Umständen sind auf den Windows Server- und Clientbetriebssystemen bereits PC/SC, CSP oder Treiber für einen Smartcardleser installiert bzw.verfügbar. Ob diese Softwarekomponenten unterstützt werden oder durch eine herstellerspezifische Software ersetzt werden müssen, erfahren Sie im Smartcard-Fachhandel.

Wichtig: Für die Verwendung von Smartcards unter Windows Vista müssen Sie die Option **Microsoft Data Protection API** in den Benutzerkonfigurationen aktivieren.

Verwenden der Identitätsprüfung

Hinweis: Um eine größere Benutzerfreundlichkeit zu erzielen, können Sie die Identitätsprüfung umgehen. Weitere Informationen finden Sie unter „Automatisches Wiederherstellen oder Aufheben der Sperrung der Anmeldeinformationen des Benutzers“ auf Seite 47.

Je nach den Einstellungen in der Benutzerkonfiguration empfiehlt es sich jedoch möglicherweise, die Identität der Benutzer in den folgenden Fällen zu prüfen:

- Der Benutzer ändert den Authentifizierungstyp, z. B. wenn zwischen der Authentifizierung mit Smartcard und mit Kennwort gewechselt wird. (Sie können eine Benutzerkonfiguration erstellen, die beim Wechsel zwischen Authentifizierungstypen lediglich eine anfängliche Prüfung erfordert. Weitere Informationen finden Sie unter „Benutzerseitiges Wechseln zwischen Authentifizierungsmethode“ im *Citrix Password Manager-Administratorhandbuch*.)
- Der Administrator ändert das primäre Kennwort eines Benutzers.
- Benutzer setzen das primäre Kennwort mit dem Konto-Self-Service zurück.
- Benutzer heben die Sperrung des Domänenkontos mit dem Konto-Self-Service auf.
- Benutzer ändern das primäre Kennwort auf einem Computer, auf dem die Agentsoftware nicht installiert ist, und melden sich dann an einem Gerät an, auf dem die Agentsoftware installiert ist.

Password Manager kann so konfiguriert werden, dass die Identität des Benutzers geprüft wird, um so sicherzustellen, dass der Benutzer zur Verwendung von Password Manager berechtigt ist. Sie können eine der beiden folgenden Methoden zur Identitätsprüfung auswählen:

Methode	Beschreibung
Altes Kennwort	Bei dieser Methode bestätigen Benutzer ihre Identität durch Eingabe des alten primären Kennwortes.
Sicherheitsfragen (auch fragenbasierte Authentifizierung genannt)	Bei dieser Methode erstellen Sie einen Fragenkatalog, der beliebig viele Fragen und Fragengruppen enthält, die Sie den Benutzern bereitstellen möchten. Sie können die von Password Manager bereitgestellten Standardfragen verwenden oder eigene Fragen erstellen. Weitere Informationen finden Sie unter „Formulieren von Sicherheitsfragen: Sicherheit und Benutzerfreundlichkeit“ im *Citrix Password Manager-Administratorhandbuch*.

Achtung: Wenn Benutzern nur das alte Kennwort als Methode zur Identitätsprüfung zur Verfügung steht, werden Benutzer, die das alte primäre Kennwort vergessen, ausgesperrt. Der Administrator muss dann in der Password Manager Console den Task zum Zurücksetzen der Benutzerdaten ausführen, damit sich die Benutzer wieder registrieren können. Möglicherweise muss der Administrator auch die Kennwörter in den Anwendungen des Benutzers zurücksetzen.

Prüfen der Benutzeridentität mit Sicherheitsfragen (fragenbasierte Authentifizierung)

Hinweis: Weitere Informationen finden Sie unter „Verwalten der fragenbasierten Authentifizierung“ im *Citrix Password Manager-Administratorhandbuch*. Wenn Sie keine Sicherheitsfragen einrichten, werden die Benutzer aufgefordert, das alte Kennwort anzugeben, wenn sie sich das erste Mal anmelden oder das primäre Kennwort ändern. Sie können Password Manager auch so konfigurieren, dass Benutzer die bevorzugte Authentifizierungsmethode (altes Kennwort oder Sicherheitsfragen) selbst auswählen können.

Password Manager ermöglicht die fragenbasierte Authentifizierung zur Prüfung der Identität des Benutzers. Hierfür stellt Password Manager vier Fragen (in Englisch, Französisch, Deutsch, Japanisch und Spanisch) zur Verfügung.

Sie können die fragenbasierte Authentifizierung in den folgenden Fällen verwenden:

- Als Teil der benutzerseitigen Registrierung der Sicherheitsfragen bei der Erstverwendung der Agentsoftware.
- Nach der Registrierung, wenn Sie die Konto-Self-Service-Funktion so konfiguriert haben, dass Benutzer die primären Anmeldeinformationen ändern oder die Sperrung der Konten aufheben können.

Wenn Benutzer die primären Kennwörter ändern, können Sie die Identität der Benutzer bestätigen, wenn Benutzer die Sicherheitsfragen im von Ihnen erstellten Fragenkatalog beantworten. Dieser Fragenkatalog wird beim ersten Starten der Agentsoftware angezeigt. Benutzer beantworten die erforderliche Anzahl der Sicherheitsfragen und werden bei bestimmten Kennwortänderungsereignissen ggf. zur erneuten Eingabe dieser Informationen aufgefordert.

Automatisches Wiederherstellen oder Aufheben der Sperrung der Anmeldeinformationen des Benutzers

Wichtig: Die automatische Schlüsselverwaltung ist nicht so sicher wie andere Methoden zur Schlüsselwiederherstellung, z. B. Sicherheitsfragen und altes Kennwort.

Sie können Password Manager so konfigurieren, dass die Identitätsprüfung umgangen wird und die Anmeldeinformationen des Benutzers (d. h. die den Benutzerdaten zugeordneten Verschlüsselungsschlüssel) automatisch wiederhergestellt werden. Hierfür müssen Sie den Password Manager-Dienst installieren und das Schlüsselverwaltungsmodul verwenden.

Der Arbeitsablauf für die automatische Schlüsselverwaltung sieht im Wesentlichen wie folgt aus:

1. Installieren Sie den Citrix Password Manager-Dienst mit dem Schlüsselverwaltungsmodul.
2. Erstellen oder bearbeiten Sie die Benutzerkonfigurationen und wählen Sie die Schlüsselwiederherstellungsmethode, die die automatische Schlüsselverwaltung ohne Identitätsprüfung ermöglicht. Diese Option ist als Teil der Eigenschaft **Sekundäre Datenschutzmethode** in der Benutzerkonfiguration verfügbar.

Siehe auch:

- „Schlüsselverwaltung“ auf Seite 60
- „Sekundäre Datenschutzoptionen auswählen“ im *Citrix Password Manager-Administratorhandbuch*
- „Aktivieren der Self-Service-Funktionen“ im *Citrix Password Manager-Administratorhandbuch*

Planen der Benutzerkonfigurationen

Wichtig: Bevor Sie Password Manager Agent den Benutzern bereitstellen, müssen Sie Benutzerkonfigurationen erstellen. Benutzerkonfigurationen enthalten die Lizenzserver- und Lizenzierungsinformationen, die von der Agentsoftware benötigt werden.

Hinweis: Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.

Eine Benutzerkonfiguration ist eine einmalige Sammlung von Einstellungen, Kennwortrichtlinien und Anwendungen, die Sie auf Benutzer anwenden, die einer Active Directory-Hierarchie (Organisationseinheit oder einzelner Benutzer) oder einer Active Directory-Gruppe zugeordnet sind (Ausnahme: Verteilergruppen und lokale Gruppen der Domäne im gemischten Modus von Active Directory, welche nicht unterstützt werden). Mit Benutzerkonfigurationen können Sie Verhalten und Darstellung der Agentsoftware für Benutzer steuern. Weitere Informationen finden Sie unter „Standardeigenschaften von Benutzerkonfigurationen“ im *Citrix Password Manager-Administratorhandbuch*

Benutzerkonfigurationen legen unter anderem die Benutzerinformationen, Anwendungsdefinitionen, Kennwortrichtlinien und Methoden zur Identitätsprüfung fest. Darüber hinaus müssen Sie in jeder Benutzerkonfiguration Lizenzierungsinformationen (Lizenzserver und Lizenztyp) angeben. Aus diesem Grund können die Benutzer die Agentsoftware erst dann verwenden, wenn Sie die entsprechenden Benutzerkonfigurationen erstellt haben.

Vor dem Erstellen von Benutzerkonfigurationen müssen Sie Folgendes erstellt bzw. definiert haben:

- Zentraler Speicher
- Dienstmodule (optional)
- Anwendungsdefinitionen
- Kennwortrichtlinien
- Sicherheitsfragen (optional)

Benutzerkonfigurationen enthalten die folgenden Elemente:

- Benutzer, die einer Active Directory-Domänenhierarchie (Organisationseinheit oder einzelner Benutzer) oder einer Gruppe zugeordnet sind.
- Datenschutzmethoden (weitere Informationen finden Sie unter „Typen der im Unternehmen verwendeten Smartcards“ auf Seite 42 und „Verwenden der Identitätsprüfung“ auf Seite 44).
- Erstellte Anwendungsdefinitionen, die Sie bei der Erstellung einer Benutzerkonfiguration in einer Anwendungsgruppe zusammenfassen können.
- Kennwortrichtlinien, die für bestimmte Anwendungsgruppen gelten. (Beim Erstellen einer Benutzerkonfiguration können Sie Anwendungsgruppen erstellen, die Sie einer Benutzerkonfiguration zuordnen. Sie können auch nach dem Erstellen einer Benutzerkonfiguration eine Anwendungsgruppe hinzufügen.)
- Self-Service-Funktionen (Kontosperrung aufheben und Kennwort zurücksetzen) und Schlüsselverwaltungsoptionen (Verwenden von alten Kennwörtern, Sicherheitsfragen, die Sie für die Benutzer erstellen, und automatische Schlüsselverwaltung).
- Einstellungen für Optionen, wie z. B. Hotdesktop, Provisioning von Anmeldeinformationen und Anwendungssupport.

Überlegungen

- Wenn Sie dieselben Einstellungen der Benutzerkonfiguration auf eine andere Benutzergruppe anwenden müssen, duplizieren Sie die Benutzerkonfiguration in der Konsole und nehmen Sie die entsprechenden Einstellungsänderungen vor.
- Die Organisation der Benutzerumgebung von Password Manager hat Einfluss auf die Funktionsweise der Benutzerkonfigurationen. Benutzerkonfigurationen werden in der Password Manager-Umgebung einer Active Directory-Hierarchie (OU oder Benutzer) oder einer Active Directory-Gruppe zugeordnet. Wenn Sie beide Optionen verwenden (Hierarchie oder Gruppe) und ein Benutzer sich in beiden Containern befindet, hat die der Hierarchie zugeordnete Benutzerkonfiguration Vorrang und wird verwendet. Bei einer solchen Konstellation spricht man von einer gemischten Umgebung.
- Die Benutzerkonfigurationsdaten im zentralen Speicher haben Vorrang vor denen im lokalen Speicher (d. h. den Benutzerdaten, die auf dem Computer eines Benutzers gespeichert sind). Die Benutzerdaten im lokalen Speicher werden in der Regel dann verwendet, wenn der zentrale Speicher nicht verfügbar oder offline ist.

Gemeinsames Verwenden von Ressourcen oder Arbeitsstationen (Hotdesktop)

Hinweis: Weitere Informationen zur Konfiguration von Hotdesktop finden Sie unter „Hotdesktop: Desktopfreigabeumgebung für Benutzer“ im *Citrix Password Manager-Administratorhandbuch*

Mit der Hotdesktop-Funktion können Benutzer Arbeitsstationen effizient und sicher gemeinsam verwenden. Hotdesktop bietet ein bequemes und schnelles Wechseln der Benutzer und Single Sign-On-Funktion mit Password Manager.

Bevor Sie Hotdesktop implementieren können, müssen Sie folgende Schritte ausführen:

- Erstellen von Hotdesktop-relevanten Konfigurationen.
- Konfigurieren eines Hotdesktop-Kontos.
- Bearbeiten der Skripte, mit denen definiert wird, welche Anwendungen auf den Hotdesktop-Geräten ausgeführt werden und wie sich diese beim Starten und Beenden verhalten.

Die Hotdesktop-Funktion wird nicht standardmäßig installiert. Sie können die Funktion bei der Agentinstallation auswählen. Bestehende Agentbereitstellungen können auch für die Verwendung von Hotdesktop aktualisiert werden.

Hinweis: Wenn Sie Hotdesktop in einer Umgebung bereitstellen, in der sich Benutzer mit Smartcards anmelden und die ausgewählte Smartcardschlüsselquelle DPAPI mit Profil ist, wählen Sie für diese Benutzer nicht **Benutzer zur Eingabe des alten Kennworts auffordern** als einzige Methode zur Schlüsselwiederherstellung aus. Benutzer in solchen Umgebungen können nicht das richtige alte Kennwort eingeben und würden somit unwiderruflich aus dem System ausgeschlossen. Wählen Sie zur Vermeidung dieses Problems die Option zur automatischen Schlüsselverwaltung aus oder stellen Sie die fragenbasierte Authentifizierung als eine Option zur Verfügung.

In diesem Abschnitt werden die folgenden Themen behandelt:

- „Steuern von Anwendungen“ auf Seite 52
- „Benutzererfahrung bei Hotdesktop“ auf Seite 52

Steuern von Anwendungen

Mit Hotdesktop werden Benutzer schnell mit den Windows-Anmelde-informationen oder einer starken Smartcard-Authentifizierungsmethode authentifiziert. Als Administrator können Sie Hotdesktop so konfigurieren, dass Anwendungen in der Hotdesktop-Umgebung gestartet werden, damit Benutzer nicht die Anwendungen suchen und auf den Anwendungsstart warten müssen.

Darüber hinaus können Sie Hotdesktop so konfigurieren, dass alle Anwendungen richtig beendet werden und die nächste Benutzersitzung in einer sauberen Umgebung gestartet wird.

Weitere Informationen finden Sie unter „Festlegen des Anwendungsverhaltens für Hotdesktop-Benutzer“ im *Citrix Password Manager-Administratorhandbuch*.

Benutzererfahrung bei Hotdesktop

Bei der Anmeldung des Hotdesktop-Kontos wird das Gerät in einen Modus für die schnelle Benutzerumschaltung gesetzt, der die Anzeige einer standard-mäßigen Windows-Authentifizierungsaufforderung auslöst. Das Hotdesktop-Konto bleibt unabhängig von der Aktivität des Hotdesktop-Benutzers angemeldet.

Wenn sich Benutzer authentifizieren, melden sie sich an Hotdesktop nicht im traditionellen Sinne an. Hotdesktop startet mit den Windows-Anmelde-informationen der Benutzer eine Hotdesktop-Sitzung. Da Benutzer nicht richtig angemeldet sondern nur authentifiziert sind, treten die zeitintensiven Ereignisse nicht auf, die normalerweise mit der Anmeldung verbunden sind, z. B. Anwenden der Gruppenrichtlinie, Initialisierung des Druckers usw. Dies führt dazu, dass Benutzer bei der Ausführung von Hotdesktop eine schnelle Benutzerumschaltung wahrnehmen. Ein Benutzer kann eine Sitzung starten, alle berufsbezogenen Aufgaben ausführen, und die Sitzung beenden, damit sich der nächste Benutzer am System anmelden und Aufgaben durchführen kann. Das Umschalten von Benutzer zu Benutzer erfolgt schnell und mühelos.

Password Manager Agent wird beim Start der Hotdesktop-Sitzung gestartet. Nach dem Herstellen der Sitzung greift Hotdesktop auf die Windows-Anmeldeinformationen des Benutzers zu und startet Anwendungen in der normalen Benutzeroberfläche. Diese Clientanwendungen fordern die Benutzer normalerweise zur Eingabe der Anmeldeinformationen auf, die von der Agentsoftware gesendet werden können. Die Agentsoftware verwendet die Einstellungen, die dem Windows-Konto zugeordnet sind.

Weitere Informationen finden Sie unter „Prozessablauf beim Starten und Beenden von Hotdesktop“ im *Citrix Password Manager-Administratorhandbuch*.

Lizenzierungsanforderungen

Citrix empfiehlt, dass Sie zuerst den Lizenzserver installieren und die Lizenzen hinzufügen, bevor Sie Password Manager installieren.

Weitere Informationen zu den Anforderungen, Bedingungen und zur Installation der Lizenzierung finden Sie im Handbuch *Schnelleinstieg für die Citrix Lizenzierung*, das auf der Website http://support.citrix.com/licensing/ unter dem Seitentitel „Top Licensing Resources“ zur Verfügung steht.

Hinweis: Links zu dem Handbuch *Schnelleinstieg für die Citrix Lizenzierung* finden Sie in der Datei Password_Manager_Read_Me_First.html und im Citrix Knowledge Center unter dem Titel „Top Licensing Resources“ auf der Seite http://support.citrix.com/licensing/.

Getrennter Modus

Hinweis: Dieser Modus wird in der Benutzerkonfiguration festgelegt. Weitere Informationen finden Sie unter „Konfigurieren der Lizenzierung“ im *Citrix Password Manager-Administratorhandbuch*.

Wenn Sie Benutzer haben, deren Verbindung zum Lizenzserver für längere Zeit getrennt ist, z. B. mobile Benutzer mit Laptops, müssen Sie für diese Benutzer einen *Zeitraum für den getrennten Modus* angeben. Der Zeitraum für den getrennten Modus wird in den Lizenzierungseinstellungen in der Benutzerkonfiguration der Agentsoftware angegeben. Der Zeitraum für den getrennten Modus gibt zwei wichtige Aspekte des Lizenzierungsverhalten an:

- Die Dauer, für die eine Benutzerverbindung zum Lizenzserver getrennt sein kann, ohne in den Lizenzierungskulanzzeitraum überzugehen. Nach dem Ablauf des Zeitraums für den getrennten Modus gehen die Benutzerverbindungen, die der Benutzerkonfiguration zugeordnet sind, in den Lizenzierungskulanzzeitraum von 30 Tagen über.

- Der Zeitraum, bis eine ausgecheckte Lizenz, die im getrennten Modus ist, an den Pool verfügbarer Password Manager-Lizenzen auf dem Lizenzserver zurückgegeben wird, unabhängig davon, ob das Produkt erneut eine Verbindung zum Lizenzserver herstellt. Wenn eine Lizenz ausgecheckt ist, und der Zeitraum für den getrennten Modus, der dieser Lizenz zugeordnet ist, vor dem Einchecken der Lizenz abläuft, checkt der Lizenzserver die Lizenz wieder ein, damit sie zur Verfügung steht. Beispiel: Wenn ein Laptop mit Password Manager verloren geht und nie wieder eine Verbindung zum Unternehmensnetzwerk herstellt, checkt der Lizenzserver die Lizenz automatisch am Ende des Zeitraums für den getrennten Modus ein.

Wenn Sie den Zeitraum für den getrennten Modus festlegen, geben Sie an, wie lange Sie warten, bis die Lizenz an den Pool der verfügbaren Lizenzen zurückgegeben wird.

Citrix empfiehlt, dass Sie lange Zeiträume für den getrennten Modus für Benutzer angeben, die nicht regelmäßig eine Verbindung zum Unternehmensnetzwerk herstellen, z. B. Verkaufsmitarbeiter, die remote arbeiten. Stellen Sie den Zeitraum auf die längste Dauer ein, die Benutzer in dieser Konfiguration keine Verbindung zum Netzwerk herstellen. Beachten Sie jedoch, dass Sie ausgecheckte Lizenzen für die Dauer dieses Zeitraums nicht wieder dem Pool hinzufügen können, selbst wenn das Gerät verloren oder kaputt ist.

Verwalten einer Umgebung mit gemischten Lizenztypen

Je nach den Password Manager-Anforderungen, die für Ihre Umgebung bzw. Ihr Unternehmen gelten, haben Sie ggf. Lizenzen für benannte Benutzer und für gleichzeitige Benutzer erworben. Sie könnten beispielsweise für mobile Benutzer, die über Desktopcomputer und Laptop auf die Agentsoftware zugreifen, Benutzerkonfigurationen nach dem Lizenzierungsmodell für benannte Benutzer erstellen. Außerdem könnten Sie Benutzerkonfigurationen nach dem Lizenzierungsmodell für gleichzeitige Benutzer erstellen, die z. B. für Hotdesktop-Benutzer gelten.

In einigen Fällen könnten alle benannten Benutzerlizenzen verwendet werden, und Password Manager steht einigen Benutzern daher nicht mehr zur Verfügung. Unter diesen Umständen können Sie gleichzeitige Benutzerlizenzen in der Benutzerkonfiguration festlegen, die offline verwendet werden.

So verwenden Sie verfügbare CCU-Lizenzen offline

1. Erstellen Sie eine Benutzerkonfiguration, wie unter „Erstellen einer Benutzerkonfiguration mit dem Assistenten für Benutzerkonfigurationen“ im *Citrix Password Manager-Administratorhandbuch* beschrieben.
2. Wählen Sie auf der Seite **Lizenzierung konfigurieren** die Option **CCU-Lizenzierung (nur Enterprise und Platinium Edition)** aus.
3. Wählen Sie die Option **Lizenzverbrauch für Offlineverwendung zulassen** aus und legen Sie fest, wie lange die Lizenz beim Lizenzserver ausgecheckt sein kann.

   Weitere Informationen finden Sie unter „Getrennter Modus“ auf Seite 54.
4. Schließen Sie die Benutzerkonfiguration ab.

Für Benutzer, die dieser Benutzerkonfiguration zugeordnet sind, ist das Lizenzierungsmodell dasselbe wie eine benannte Benutzerlizenz. Die Lizenz kann von Benutzern verwendet werden, die gelegentlich remote arbeiten und über längere Zeiträume hinweg offline sind. Gleichzeitige Benutzerlizenzen werden dann pro Benutzer verbraucht.

Auswählen optionaler Funktionen des Password Manager-Dienstes

Der Password Manager-Dienst ist ein Webdienst, der die Daten, die vom Password Manager-Dienst, der Konsole und dem Agent verwendet werden, mit SSL (Secure Sockets Layers) verschlüsselt. Der Dienst verwendet einen dedizierten Webserver als Host für die optionalen Funktionen von Password Manager.

Installieren Sie den Password Manager-Dienst, wenn Sie eines oder mehrere der folgenden Module implementieren möchten:

- Self-Service: Mit diesem Modul können Benutzer über die Schaltfläche **Konto-Self-Service** im Windows-Anmeldedialogfeld die Active Directory-Kennwörter zurücksetzen und die Kontosperrung aufheben.
- Datenintegrität: Mit diesem Modul können Daten vor der Übertragung vom zentralen Speicher zur Agentsoftware digital signiert werden.
- Schlüsselverwaltung: Mit diesem Modul können sich Benutzer am Netzwerk anmelden und sofort auf die von Password Manager verwalteten Anwendungen zugreifen, ohne dass die Benutzeridentität durch fragenbasierte Authentifizierung geprüft wird.
- Provisioning: Mit diesem Modul können Sie in der Konsole Anmeldeinformationen der Benutzer hinzufügen, entfernen oder aktualisieren.
- Synchronisierung der Anmeldeinformationen: Mit diesem Modul können Benutzer die Anmeldeinformationen zwischen verschiedenen Konten synchronisieren (auch Kontozuordnung genannt).

Wichtig: Der Server mit dem Password Manager-Dienst enthält sehr vertrauliche Benutzerdaten. Sie sollten einen dedizierten Server verwenden, der an einem physisch sicheren Standort installiert ist.

Konto-Self-Service

Hinweis: Sie können den Konto-Self-Service nur in einer Active Directory-Umgebung verwenden, um die benutzerseitige Zurücksetzung des primären Kennwortes sowie die Aufhebung der Sperrung der Windows-Domänenkonten zu ermöglichen.

Sie können in den Self-Service-Funktionen von Password Manager konfigurieren, dass Benutzer ohne Beteilung des Administrators oder des Helpdeskpersonals das primäre Kennwort zurücksetzen oder die Sperrung der Windows-Domänenkonten aufheben können. Je nach Bedarf können Sie eine oder beide Konto-Self-Service-Funktionen (Kennwort zurücksetzen und Kontosperrung aufheben) sicher in der Password Manager-Umgebung implementieren.

Das benutzerseitige Zurücksetzen des Kennworts ermöglicht es Benutzern, die ihr primäres Kennwort vergessen haben, das Kennwort rückzusetzen und die Sperrung der eigenen Konten aufzuheben. Mit der Funktion zum Aufheben der Kontosperrung können Benutzer die Sperrung der Domänenkonten aufheben, wenn sie ausgesperrt wurden.

Diese Kontofunktionen werden durch die fragenbasierte Authentifizierung geschützt. So wird sichergestellt, dass Benutzer zum Zurücksetzen der Kennwörter oder Aufheben der Kontosperrung berechtigt sind. Weitere Informationen finden Sie unter „Verwenden der Identitätsprüfung“ auf Seite 44.

Wenn Benutzer den Konto-Self-Service aktivieren, müssen sie sich registrieren und die Sicherheitsfragen beantworten, die Sie erstellt und ausgewählt haben. Diese Sicherheitsfragen werden den Benutzern angezeigt, wenn sie das Kennwort zurücksetzen oder die Sperrung des Kontos aufheben möchten. Werden die Fragen richtig beantwortet, können die Benutzer die Kennwörter zurücksetzen oder die Kontosperrung aufheben.

Der Konto-Self-Service kann auch mit dem Webinterface verwendet werden. Das Webinterface ist eine Komponente von Citrix Presentation Server, mit der Benutzer auf veröffentlichte Anwendungen zugreifen können, indem sie auf die Verknüpfungen in einer Webseite klicken.

Datenintegrität

Hinweis: Wenn Sie bereits einen Sicherheitsrahmen implementiert haben, mit dem die gesendeten Daten geschützt werden, z. B. IPsec (Internet Protocol Security) oder SMB-Signatur (Server Message Block), brauchen Sie das Modul **Datenintegrität** nicht zu installieren.

Installieren Sie das Modul **Datenintegrität**, wenn Sie sicherstellen möchten, dass die in den Komponenten von Password Manager übertragenen Daten von einer sicheren und autorisierten Quelle stammen. Dieses Modul ist optional und für Benutzer gedacht, die keine vertrauenswürdigen Netzwerke haben.

Das Modul **Datenintegrität** enthält die Dateien mit den öffentlichen und privaten Schlüsseln, die für das Signieren von Daten verwendet werden. Das Modul verwendet veröffentlichte Schlüsselkryptografie (RSA), um sicherzustellen, dass die Agentsoftware nur Konfigurationsdaten erhält, die von einer autorisierten Quelle stammen.

Wichtig: Das Modul **Datenintegrität** verteilt nie den privaten Schlüssel.

Nach der Signatur der Daten sendet die Konsole die Daten und die Signatur an den zentralen Speicher. Bei der Synchronisierung erhält der Agent die Daten und die Signatur vom zentralen Speicher. Der Agent kontaktiert dann den Password Manager-Dienst, um eine Kopie des öffentlichen Schlüssels zu erhalten, der zur Prüfung der Signatur benötigt wird, die vom zentralen Speicher empfangen wurde.

Wenn der Agent für die Verwendung des Moduls **Datenintegrität** konfiguriert ist, werden alle Daten abgelehnt, die die Prüfung der Datenintegrität nicht bestanden haben. Wenn eine Prüfung fehlschlägt, protokolliert der Agent das Ereignis und zeigt den Benutzern eine Fehlermeldung an, in der sie aufgefordert werden, sich an den Administrator zu wenden. Die Agentsoftware verwendet dann standardmäßig vorherige Konfigurationen oder kehrt in einen Offlinestatus zurück.

Schlüsselverwaltung

Mit der Schlüsselverwaltung melden sich Benutzer am Netzwerk an und können sofort ohne fragenbasierte Authentifizierung auf die von Password Manager verwalteten Anwendungen zugreifen. (Dieses Schema wird auch als automatische Schlüsselverwaltung bezeichnet.) Wenn Benutzer die primären Kennwörter ändern, erkennt der Agent die Kennwortänderungen und stellt die Verschlüsselungsschlüssel der Benutzer mit dem Password Manager-Dienst wieder her.

Die automatische Schlüsselverwaltung stellt für Benutzer die einfachste und schnellste Zugriffsmethode auf die verwendeten Anwendungen dar. Allerdings schützt die automatische Schlüsselverwaltung nicht vor einem unbefugten Benutzer oder Administrator, der die Identität eines Benutzers annimmt, da es kein nur dem Benutzer bekanntes Geheimnis gibt, mit dem das Netzwerkkennwort des Benutzers geschützt wird. Um dieses potenzielle Problem zu vermeiden, sollten Sie die automatische Schlüsselverwaltung zusammen mit dem Konto-Self-Service-Modul und der fragenbasierten Authentifizierung implementieren.

Die automatische Schlüsselverwaltung verwendet die *Schlüsselaufteilung* (das Aufteilen eines privaten Schlüssels in zwei Teile), um Sicherheitsrisiken zu verringern.

Wichtig: Abhängig von der Sicherheitsrichtlinie der Organisation können Systemadministratoren auf Kennwörter für von Password Manager verwaltete Anwendungen zugreifen. Überprüfen Sie die Sicherheitsrichtlinie der Organisation, bevor Sie Password Manager die Handhabung von Kennwörtern erlauben, die Benutzer eigentlich vollständig vertraulich halten möchten. Das Deaktivieren von automatischen Schlüsselverwaltungsfunktionen in der Einstellung **Datenschutzmethoden** der Benutzerkonfiguration kann ebenfalls zur Vermeidung von nicht autorisierten Zugriffen beitragen. Weitere Informationen finden Sie unter „Annahme der Identität des Benutzers“ auf Seite 67 und „Datenschutzmethoden auswählen“ sowie „Sekundäre Datenschutzoptionen auswählen“ im *Citrix Password Manager-Administratorhandbuch*.

Provisioning

Hinweis: Weitere Informationen zum Provisioning finden Sie unter „Automatisieren der Eingabe der Anmeldeinformationen mit dem Provisioning“ im *Citrix Password Manager-Administratorhandbuch*.

Das Provisioning (Provisioning von Anmeldeinformationen) steigert die Flexibilität und erweitert die Funktionen von Password Manager in der Unternehmensumgebung, da Sie mehrere zeitintensive Prozesse automatisieren können. Bei der Bereitstellung einer neuen Password Manager-Installation, dem Hinzufügen von Hunderten von Benutzern und neuen Anwendungen oder dem Entfernen nicht benötigter Informationen verkürzt das Provisioning den Zeitaufwand für diese Aufgaben.

Beispiel: Sie können mit dem Provisioning alle Benutzernamen und Kennwörter für alle Anwendungen dem zentralen Speicher hinzufügen. Dann müssen die Benutzer bei der Erstverwendung der Software nicht die *Ersteinrichtung der Anmeldeinformationen* durchlaufen. Wenn Sie die Bereitstellung neuer Software für die Benutzer planen, können Sie einfach eine Anwendungsdefinition für die Anwendung erstellen und mit dem Provisioning die Anmeldeinformationen aller Benutzer hinzufügen, die diese Anwendung verwenden.

Das Provisioning ermöglicht Folgendes:

- Hinzufügen, Ändern und Löschen von Anmeldeinformationen im zentralen Speicher
- Zurücksetzen der Anmeldeinformationen der Benutzer
- Entfernen von Benutzern und den entsprechenden Anmeldeinformationen für die Anwendung von Password Manager

Das Provisioning von Anmeldeinformationen wird erreicht, wenn Sie mit den Informationen über die Umgebung eine Vorlage erstellen, mit der Sie Anmeldeinformationen im zentralen Speicher hinzufügen, entfernen oder ändern können. Das Provisioning von Anmeldeinformationen wird im Rahmen des Password Manager-Dienstes verarbeitet.

Synchronisierung der Anmeldeinformationen (Kontozuordnung)

Weitere Informationen finden Sie unter „Verwenden der Kontozuordnung mit mehreren zentralen Speichern und Kontoanmeldeinformationen der Benutzer in einem Unternehmen mit mehreren Domänen“ auf Seite 30 und „Synchronisieren von Anmeldeinformationen mit der Kontozuordnung“ im *Citrix Password Manager-Administratorhandbuch*.

Mit der Kontozuordnung kann sich ein Agentbenutzer mit jedem Windows-Konto des Benutzers an jeder Anwendung anmelden. Da Password Manager normalerweise Anmeldeinformationen des Benutzers mit einem Konto verbindet, werden die Anmeldeinformationen nicht automatisch zwischen mehreren Konten des Benutzers synchronisiert. Allerdings kann der Administrator die Kontozuordnung zum Synchronisieren der Anmeldeinformationen des Benutzers konfigurieren. Benutzer, für die die Kontozuordnung konfiguriert ist, können mit jedem ihrer Konten in der Password Manager-Umgebung auf alle Anwendungen zugreifen. Wenn die Anmeldeinformationen des Benutzers geändert, hinzugefügt oder von einem Konto entfernt werden, werden die Anmeldeinformationen automatisch mit jedem zugeordneten Konto des Benutzers synchronisiert.

Bereitstellungsszenarios für Password Manager Agent

Wie Sie Password Manager implementieren, hängt größtenteils davon ab, wie Benutzer auf Anwendungen im Unternehmen zugreifen. In einer Presentation Server-Umgebung können Sie z. B. Password Manager Agent auf jedem Server in der Farm veröffentlichen, die aktuell Anwendungen hostet, für die Authentifizierung erforderlich ist. Benutzer greifen über Citrix Verbindungen auf diese Anwendungen zu.

Wenn Benutzer Anwendungen lokal auf Arbeitsstationen, Laptops, Handheld-computern oder anderen Clientgeräten ausführen, wird die Agentsoftware auf diesen Geräten lokal installiert. In diesem Fall stellt die Agentsoftware die Anmeldeinformationen sowie den Zugriff auf die lokal auf dem Clientgerät ausgeführten Anwendungen bereit.

Die Agentsoftware kann auch in einer gemischten Umgebung mit lokalen und von Presentation Server veröffentlichten Anwendungen implementiert werden. Die lokal installierte Agentsoftware stellt die Anmeldeinformationen für die auf dem Clientgerät installierten Anwendungen zur Verfügung, während Presentation Server die Anmeldeinformationen für die veröffentlichten Anwendungen bereitstellt.

Falls zusätzlich Access Gateway Advanced Edition ausgeführt wird, werden Anwendungen von Presentation Server über einen Webbrowser bereitgestellt.

Password Manager kann mit der folgenden Software verwendet werden:

- Access Gateway Advanced Edition
- Citrix Presentation Server-Funktionen, u. a.:
    - Webinterface
    - Citrix Presentation Server Clients für Windows

Überlegungen zu Presentation Server

- Wenn Sie Password Manager in einer Presentation Server-Umgebung einsetzen, müssen Sie die Agentsoftware auf jedem Server installieren, auf dem Anwendungen veröffentlicht sind, die eine Authentifizierung erfordern. Die Agentsoftware stellt nur Anmeldeinformationen für veröffentlichte Anwendungen bereit.
- Installieren Sie die Konsole auf einem Desktop oder einem Server, der nicht zur Serverfarm gehört. Dieser Desktop oder Server sollte unter demselben Betriebssystem wie die Server ausgeführt werden, auf denen die Anwendungen veröffentlicht sind, oder unter dem Betriebssystem der Server, auf denen die Agentsoftware installiert ist. Verwenden Sie die Konsole, um Benutzerkonfigurationen zum Steuern des Agentverhaltens zu erstellen.
- Benutzer greifen mit einem Client über ICA-Verbindungen auf die in der Serverfarm veröffentlichten Anwendungen zu. Wenn ein Benutzer versucht, eine Verbindung zu einer veröffentlichten Anwendung herzustellen, die Anmeldeinformationen erfordert, erkennt der Agent die Anfrage nach den Anmeldeinformationen, die der Server mit Presentation Server sendet. Der Agent stellt den Anwendungstyp fest (Windows, Web oder hostbasiert) und ruft die entsprechenden Anmeldeinformationen von dem im Benutzerprofil gespeicherten lokalen Speicher der Anmeldeinformationen ab.

Richtlinien für mehrere primäre Authentifizierungsmethoden und Methoden zum Schutz der Anmeldeinformationen der Benutzer

Beim Erstellen einer Benutzerkonfiguration können Sie abhängig von dem im Unternehmen verwendeten Authentifizierungsschema verschiedene Methoden zum Schutz der Anmeldeinformationen des Benutzers auswählen.

Mit den folgenden Eigenschaften-Dialogfeldern der Benutzerkonfiguration optimieren Sie das Verhalten von Password Manager Agent und passen die Methode zum Schutz der Anmeldeinformationen an, wenn Benutzer eine oder mehrere primäre Authentifizierungsmethoden implementieren.

Hinweis: Weitere Informationen zum Erstellen einer Benutzerkonfiguration finden Sie unter „Erstellen einer Benutzerkonfiguration mit dem Assistenten für Benutzerkonfigurationen im *Citrix Password Manager-Administratorhandbuch*. Weitere Informationen zu diesen Optionen finden Sie unter „Datenschutzmethoden auswählen“ und „Sekundäre Datenschutzoptionen auswählen“ im *Citrix Password Manager-Administratorhandbuch*.

- „Dialogfeld „Datenschutzmethoden““ auf Seite 65
- „Dialogfeld „Sekundäre Datenschutzmethode““ auf Seite 66
- „Sicherheit und Benutzerfreundlichkeit“ auf Seite 66
- „Benutzername und Kennwort“ auf Seite 68
- „Smartcards mit Zertifikaten und Authentifizierungsdaten der Benutzer“ auf Seite 69
- „Smartcards mit PINs“ auf Seite 71
- „Servergespeicherte Profile (Microsoft DPAPI)“ auf Seite 72
- „Leere Kennwörter“ auf Seite 74

Dialogfeld „Datenschutzmethoden“

Im Eigenschaften-Dialogfeld für die Benutzerkonfiguration **Datenschutzmethoden** können Sie als Datenschutzmethode eine oder mehrere primäre Authentifizierungsmethoden auswählen. Darüber hinaus können Sie auch den Administratorzugriff auf die Anmeldeinformationen des Benutzers steuern, um zu verhindern, dass Administratoren die Identität eines Benutzers annehmen und unberechtigt auf Benutzerdaten zugreifen.

Dialogfeld „Sekundäre Datenschutzmethode“

Wenn Benutzer die primäre Authentifizierung ändern (z. B. ein Domänenkennwort ändern oder eine Smartcard ersetzen), können Sie zum Erhöhen der Sicherheit im Eigenschaften-Dialogfeld der Benutzerkonfiguration eine **Sekundäre Datenschutzmethode** festlegen, dass sich die Benutzer neu authentifizieren und einer Identitätsprüfung unterziehen müssen, bevor die Sperrung der Anwendungsanmeldeinformationen aufgehoben wird.

Sicherheit und Benutzerfreundlichkeit

Um zu entscheiden, welche Optionen Sie in den beiden Dialogfeldern für diese Benutzerkonfigurationseigenschaften auswählen, stellen Sie sich die folgenden beiden Fragen:

- Welche Authentifizierungstypen werden in der Umgebung für die Benutzer verwendet, die Sie mit dieser Benutzerkonfiguration verwalten?
- Wie können die Sicherheitsanforderungen des Unternehmens und eine umfassende Benutzerfreundlichkeit miteinander in Einklang gebracht werden?

Bedenken Sie auch, dass die folgenden Optionen sich nicht gegenseitig ausschließen und Sie verschiedene Möglichkeiten im Unternehmen miteinander kombinieren können (mehrere primäre Authentifizierungsmethoden). Ihre Entscheidung hängt letztendlich davon ab, wie stark Sie die Sicherheit der Benutzer im Unternehmen gegenüber der Benutzerfreundlichkeit gewichten.

Annahme der Identität des Benutzers

Wenn Sie den Zugriff des Administrators auf die Anmeldeinformationen des Benutzers unterbinden möchten, wählen Sie für die folgende Option **Ja** aus. Die Anmeldeinformationen sind nun vor Administratoren geschützt, die die Identität eines Benutzers annehmen und auf Benutzerdaten zugreifen möchten.

Administratorkontozugriff auf Benutzerdaten steuern

Die Standardeinstellung im Dialogfeld **Datenschutzmethoden** ist **Ja**. Bei dieser Einstellung hat der Kontoadministrator oder ein anderer Administrator keinen Zugriff auf die Kennwörter oder Daten der Benutzer. Damit wird verhindert, dass ein Administrator die Identität eines Benutzers annimmt. Mit dieser Standardeinstellung kann der Administrator sich nicht als Benutzer anmelden und möglicherweise auf Daten zugreifen, die im lokalen Speicher der Anmeldeinformationen des Benutzers gespeichert sind.

Die Einstellung **Ja** deaktiviert die Option **Microsoft Data Protection API** in diesem Dialogfeld und die Option **Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt** in dem folgenden Dialogfeld **Sekundäre Datenschutzmethode**. Smartcards und servergespeicherte Profile sind in diesem Fall nicht zugelassen, und Anmeldeinformationen werden bei einer Kennwortänderung ohne Authentifizierung oder Identitätsprüfung nicht automatisch wiederhergestellt.

Wählen Sie **Nein**, wenn Sie alle Optionen für mehrere Authentifizierungen in diesem Dialogfeld und dem nächsten Dialogfeld **Sekundäre Datenschutzmethode** verwenden möchten (einschließlich der Möglichkeit, Anmeldeinformationen ohne eine erneute Authentifizierung oder Identitätsprüfung automatisch wiederherzustellen).

Benutzername und Kennwort

Im Dialogfeld **Datenschutzmethoden** ist standardmäßig die einfachste Implementierung ausgewählt, nämlich eine Umgebung, in der nur ein Kennwort erforderlich ist. Bei dieser Standardeinstellungen verwenden Benutzer einfach den Benutzernamen und das Kennwort zum Schutz der Anmeldeinformationen vor nicht autorisiertem Zugriff durch Administratoren.

Wichtig: Die Sicherheit dieser Methode hängt von der relativen Stärke der Domänenkennwortrichtlinie ab. Je strenger (oder komplexer) die Anforderungen an das Kennwort sind, desto sicherer ist diese Methode.

Option	Beschreibung
Administratorkontozugriff auf Benutzerdaten steuern	Weitere Informationen finden Sie unter „Annahme der Identität des Benutzers“ auf Seite 67.
Authentifizierungsdaten der Benutzer	Ausgewählt. Um auf die Benutzerdaten zuzugreifen und sie zu schützen, wird ein nur dem Benutzer bekanntes Geheimnis verwendet. In diesem Fall handelt es sich bei dem Geheimnis um ein Kennwort. Die Kennwortsicherheit ergibt sich aus dem Domänenkennwort, das der Benutzer eingegeben hat, oder einem einmaligen Kennwort aus Tokens, Proximitykarten oder biometrischen Geräten.

Smartcards mit Zertifikaten und Authentifizierungsdaten der Benutzer

Wichtig: Diese Option wird von Password Manager Agent Version 4.1 nicht unterstützt. Wählen Sie **Datenschutz wie in Password Manager 4.1 und vorherigen Versionen verwenden** und **Smartcard-Datenschutz**, wenn Sie diese Legacyversionen der Agentsoftware verwenden möchten. Weitere Informationen finden Sie unter „Datenschutzmethoden auswählen“ im *Citrix Password Manager-Administratorhandbuch*.

Wichtig: Für die Verwendung von Smartcards unter Windows Vista müssen Sie die Option **Microsoft Data Protection API** in den Benutzerkonfigurationen aktivieren.

Wählen Sie diese Option, wenn Sie im Unternehmen Smartcards mit eingebetteten Zertifikaten oder digitalen Signaturen und Authentifizierungsdaten der Benutzer kombinieren möchten. Die Kombination von Smartcards mit einem Benutzernamen und Kennwort für die Authentifizierung ist die sicherste Methode zum Schutz von Authentifizierungsdaten der Benutzer. Wenn Sie servergespeicherte Profile auf Arbeitsstationen speichern, lesen Sie die Informationen zur erforderlichen Optionsauswahl unter „Servergespeicherte Profile (Microsoft DPAPI)“ auf Seite 72.

Hinweis: Wählen Sie die Option **Smartcardzertifikat** aus, wenn Sie Smartcards mit Hotdesktop verwenden.

Option	Beschreibung
Administratorkontozugriff auf Benutzerdaten steuern	Weitere Informationen finden Sie unter „Annahme der Identität des Benutzers“ auf Seite 67.
Authentifizierungsdaten der Benutzer	**Ausgewählt.** Um auf die Benutzerdaten zuzugreifen und sie zu schützen, wird ein nur dem Benutzer bekanntes Geheimnis verwendet. In diesem Fall handelt es sich bei dem Geheimnis um ein Kennwort. Die Kennwortsicherheit ergibt sich aus dem Domänenkennwort, das der Benutzer eingegeben hat, oder einem einmaligen Kennwort aus Tokens, Proximitykarten oder biometrischen Geräten.
Smartcardzertifikat	**Ausgewählt.** In diesem Fall ist das nur dem Benutzer bekannte Geheimnis durch die von dem Sicherheitszertifikat der Smartcard bereitgestellte Ver- und Entschlüsselung geschützt.

Smartcards mit PINs

Hinweis: Diese Option wird von Password Manager Agent Version 4.1 unterstützt, wenn Sie bei Verwendung der Legacyversionen der Agentsoftware **Datenschutz wie in Password Manager 4.1 und vorherigen Versionen verwenden** und **PIN-Nummer als Kennwort** auswählen.

Wenn Sie Smartcards verwenden, die keine Sicherheitszertifikate als primäre Authentifizierung in Windows-Domänen unterstützen, oder wenn Sie keine servergespeicherten Profile verwenden, wählen Sie die Option **Smartcard-PINs zulassen**. Wenn diese Option gewählt wurde, werden die Verschlüsselungsschlüssel für den Schutz der sekundären Anmeldeinformationen aus der PIN der Smartcard abgeleitet.

Achten Sie darauf, dass starke PIN-Nummern verwendet werden. In manchen Unternehmen werden als PIN vierstellige Zahlen verwendet; diese bieten einen weniger starken Schutz als beispielsweise längere Kennwörter. Citrix empfiehlt die Verwendung der Option **PIN-Nummer als Kennwort** nur dann, wenn die PINs sowohl aus Ziffern als auch aus Buchstaben bestehen und eine Mindestlänge von acht Zeichen haben.

Option	Beschreibung
Administratorkontozugriff auf Benutzerdaten steuern	Weitere Informationen finden Sie unter „Annahme der Identität des Benutzers“ auf Seite 67.
Authentifizierungsdaten der Benutzer	Ausgewählt. Um auf die Benutzerdaten zuzugreifen und sie zu schützen, wird ein nur dem Benutzer bekanntes Geheimnis verwendet. In diesem Fall handelt es sich bei dem Geheimnis um eine persönliche Identifikationsnummer (PIN).
Smartcard-PINs zulassen	Ausgewählt. Die PIN-Nummer der Smartcard wird als das nur dem Benutzer bekannte Geheimnis verwendet, um die Benutzerdaten zu schützen. Verwenden Sie diese Option nur, wenn die Richtlinien des Unternehmens bzw. die Umgebung starke PINs fordern.

Servergespeicherte Profile (Microsoft DPAPI)

Wichtig: Für die Verwendung von Smartcards unter Windows Vista müssen Sie die Option **Microsoft Data Protection API** in den Benutzerkonfigurationen aktivieren.

Hinweis: Diese Methode wird von Password Manager Agent Version 4.1 sowie von den Plattformen von Windows XP, Windows 2000 und Windows Server 2003 unterstützt. Wählen Sie **Datenschutz wie in Password Manager 4.1 und vorherigen Versionen verwenden** und **DPAPI mit Profil**, wenn Sie Legacyversionen der Agentsoftware verwenden möchten.

Wählen Sie für **Administratorkontozugriff auf Benutzerdaten steuern** die Einstellung **Nein** aus, um die Verwendung von servergespeicherten Profilen und Microsoft Data Protection API in der Umgebung zu ermöglichen. Diese Option ist die zweitsicherste Option nach „Smartcards mit Zertifikaten und Authentifizierungsdaten der Benutzer“ auf Seite 69.

Wählen Sie diese Option aus, wenn Sie servergespeicherte Profile zur Implementierung eines Kerberos-Netzwerkauthentifizierungsprotokolls für Benutzer verwenden. Diese Option funktioniert nur, wenn servergespeicherte Profile vorhanden sind. Wenn Sie servergespeicherte Profile auf Arbeitsstationen speichern, müssen Sie diese Option auswählen.

Password Manager leitet die Verschlüsselungsschlüssel für den Schutz der sekundären Anmeldeinformationen aus dem primären Kennwort des Benutzers ab. Wenn jedoch ein Benutzer eine Smartcard für die primäre Authentifizierung verwendet, gibt es kein primäres Kennwort. Somit kann es auch nicht verwendet werden. In diesem Fall ist die beste Option im Agent Microsoft Data Protection API. Diese Option verwendet die Microsoft DPAPI, um die Verschlüsselungsschlüssel abzuleiten und die sekundären Anmeldeinformationen zu schützen. Diese Verschlüsselungsmethode verwendet die Windows- oder Domänenanmeldeinformationen des Benutzers zum Ermitteln der Verschlüsselungsschlüssel.

Wenn Benutzer mit Kennwörtern auf den Computer und mit einem Kerberos-Netzwerkauthentifizierungsprotokoll auf Server mit Citrix Presentation Server zugreifen, wählen Sie die folgenden Optionen:

- **Nein** für **Administratorkontozugriff auf Benutzerdaten steuern**
- **Authentifizierungsdaten der Benutzer**
- **Microsoft Data Protection API**

Mit dieser Methode können Benutzer sich auch mit Anmeldeinformationen und Smartcards anmelden. Weitere Informationen finden Sie unter „Smartcards mit Zertifikaten und Authentifizierungsdaten der Benutzer“ auf Seite 69.

Leere Kennwörter

Wichtig: Wenn Sie diese Option nicht auswählen und ein leeres Kennwort in der Umgebung zulässig ist, kann die Agentsoftware kein nur dem Benutzer bekanntes Geheimnis ermitteln und keine weiteren Datenschutzmaßnahmen mit dem leeren Kennwort vornehmen.

Das Zulassen von leeren Kennwörtern sollte als Spezialfall angesehen und *nur in Umgebungen mit geringen Sicherheitsanforderungen verwendet werden, die aber extrem benutzerfreundlich sein sollen*. Ein denkbares Szenario ist z. B., wenn ein normaler PC oder eine Arbeitsstation in einer Fabrikhalle aufgestellt und von vielen Benutzern verwendet wird. Password Manager kann nach wie vor verwendet werden, um den Zugriff auf Anwendungen zu steuern, aber die Anmeldeinformationen der Benutzer für den Zugriff auf die Arbeitsstation enthalten ein leeres Kennwort.

Option	Beschreibung
Administratorkontozugriff auf Benutzerdaten steuern	Weitere Informationen finden Sie unter „Annahme der Identität des Benutzers“ auf Seite 67.
Authentifizierungsdaten der Benutzer	**Ausgewählt.** Um auf die Benutzerdaten zuzugreifen und sie zu schützen, wird ein nur dem Benutzer bekanntes Geheimnis verwendet. In diesem Fall handelt es sich bei dem Geheimnis um ein Kennwort.
Schutz mit leeren Kennwörtern zulassen	**Ausgewählt.** Wenn Sie diese Option auswählen und die Agentsoftware ein leeres Kennwort bei einem Benutzer entdeckt, wird zum Schutz der Daten ein nur dem Benutzer bekanntes Geheimnis aus der Benutzer-ID ermittelt.

Installieren von Password Manager

In diesem Abschnitt werden die Aufgaben beschrieben, die zur Installationsvorbereitung, Installation und Konfiguration von Citrix Password Manager erforderlich sind:

- „Zusammenfassung der Installationsschritte“ auf Seite 76
- „Hardware- und Softwareanforderungen“ auf Seite 77
- „Sicherheits- und Kontoanforderungen für den Password Manager-Dienst“ auf Seite 81
- „Kontoanforderungen zum Installieren und Verwenden von Password Manager“ auf Seite 86
- „Installieren von Microsoft .NET 2.0 Framework“ auf Seite 88
- „Installieren von Java Runtime Environment“ auf Seite 90
- „Lizenzierungsanforderungen“ auf Seite 92
- „Vor der Installation von Password Manager“ auf Seite 93
- „Erstellen eines zentralen Speichers“ auf Seite 96
- „Erstellen eines zentralen Speichers an einer Befehlszeile (optional)“ auf Seite 99
- „Installieren und Konfigurieren des Password Manager-Dienstes“ auf Seite 106
- „Installieren und Konfigurieren der Password Manager Console“ auf Seite 113
- „Installieren und Konfigurieren von Password Manager Agent“ auf Seite 117
- „Installation von Password Manager Agent ohne Benutzereingriffe“ auf Seite 126

Zusammenfassung der Installationsschritte

Aufgabe	Siehe Abschnitt oder Dokument
Vorbereitungen zur Installation	
Legen Sie fest, auf welchen Computern in der Umgebung die Software installiert wird.	• „Planen der Password Manager-Umgebung“ auf Seite 19 • „Hardware- und Softwareanforderungen“ auf Seite 77
Bereiten Sie die Computer für die Installation vor.	• „ASP.NET-Anforderungen“ auf Seite 80 • „Sicherheits- und Kontoanforderungen für den Password Manager-Dienst“ auf Seite 81 • „Installieren von Microsoft .NET 2.0 Framework“ auf Seite 88 • „Installieren von Java Runtime Environment“ auf Seite 90
Installieren Sie den Lizenzserver und fügen Sie Lizenzen für Password Manager hinzu.	• „Lizenzierungsanforderungen“ auf Seite 92 • Handbuch *Schnelleinstieg für die Citrix Lizenzierung*, das unter http://support.citrix.com/licensing/ unter "Top Licensing Resources" zur Verfügung steht.
Installation	
Prüfen Sie das Menü **Autorun**.	„Vor der Installation von Password Manager“ auf Seite 93
Erstellen Sie einen zentralen Speicher.	• „Auswählen des Typs des zentralen Speichers“ auf Seite 23 • „Erstellen eines zentralen Speichers“ auf Seite 96
Installieren Sie den Password Manager-Dienst.	„Installieren und Konfigurieren des Password Manager-Dienstes“ auf Seite 106
Installieren Sie die Password Manager Console.	„Installieren und Konfigurieren der Password Manager Console“ auf Seite 113
Installieren Sie Password Manager Agent.	„Installieren und Konfigurieren von Password Manager Agent“ auf Seite 117

Hardware- und Softwareanforderungen

Wichtig: Installieren Sie Password Manager nicht auf Domänencontrollern. Das Installieren einer Komponente von Password Manager (Agent, Dienst, Konsole oder zentraler Speicher) auf einem Domänencontroller wird nicht unterstützt.

In diesem Abschnitt werden die Hardware- und Softwareanforderungen für Ihre Password Manager-Umgebung beschrieben. Dafür wird vorausgesetzt, dass jeder Computer die hardwarebezogenen Mindestanforderungen für das installierte Betriebssystem erfüllt.

Erforderliche unterstützende Systemsoftware

Unter Umständen wird für Computer in der Password Manager-Umgebung folgende unterstützende Systemsoftware benötigt.

Softwarekomponente	Erforderlich für	Bezugsquelle
Microsoft Windows Installer 3.0 oder höher	Alle	• Ordner **Support** auf der Password Manager-CD • http://www.microsoft.com
Microsoft .NET Framework 2.0	• Password Manager-Dienst • Password Manager Console • Anwendungsdefinitionstool	Ordner **Support** auf der Password Manager-CD
Java 2 Standard Edition (J2SE) Runtime Environment Version 5.0	Bei erforderlicher Unterstützung von Java-Anwendungen: • Password Manager Console • Anwendungsdefinitionstool • Password Manager Agent	• Ordner **Support** auf der Password Manager-CD • http://www.java.com
Microsoft Internet Explorer Version 6.0 oder 7.0 (nicht geschützter Modus)	Benutzer mit Zugriff auf Single Sign-On-aktivierte Webanwendungen	http://www.microsoft.com

Anforderungen für die Password Manager Console und Password Manager Agent

In dieser Tabelle sind die Software- und Hardwareanforderungen für die Password Manager Console und für Password Manager Agent aufgeführt.

Hinweis: Sie können das Anwendungsdefinitionstool für Password Manager auf jedem Computer in der Umgebung installieren, ohne die vollständige Konsole installieren zu müssen.

Password Manager-Komponenten	Unterstützte Umgebung oder Microsoft Windows-Betriebssystem	Hardware-anforderungen
Zentraler Speicher	• Active Directory • NTFS-Dateifreigabe • Freigegebener Novell Ordner	• 30 KB Speicherplatz auf der Festplatte pro Benutzer
Konsole	• Microsoft Windows XP Professional, Service Pack 2 (32 Bit) • Microsoft Windows XP Professional x64 Edition (64 Bit) • Microsoft Windows 2000 Professional, Service Pack 4 • Microsoft Windows Server 2003, Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64 Bit) • Microsoft Windows Server 2003 mit Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64 Bit) • Microsoft Windows 2000 Server, Service Pack 4 (Windows 2000 Server, Advanced Server, Datacenter Server) (32 Bit)	• 64 MB RAM • 60 MB Speicherplatz auf der Festplatte

Password Manager-Komponenten	Unterstützte Umgebung oder Microsoft Windows-Betriebssystem	Hardware-anforderungen
Agentsoftware	• Windows Vista (Business Edition, Ultimate Edition, Enterprise Edition) (32 Bit und 64 Bit • Microsoft Windows XP Professional, Service Pack 2 (32 Bit) • Microsoft Windows XP Professional x64 Edition (64 Bit) • Microsoft Windows XP Embedded • Microsoft Windows 2000 Professional, Service Pack 4 • Windows Windows Fundamentals for Legacy PCs • Microsoft Windows Server 2003, Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64 Bit) • Microsoft Windows Server 2003 mit Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit und 64 Bit) • Microsoft Windows 2000 Server, Service Pack 4 (Windows 2000 Server, Advanced Server, Datacenter Server) (32 Bit)	• 10 MB RAM • 25 MB Speicherplatz auf der Festplatte (keine Installation der optionalen Funktionen) • 35 MB Speicherplatz auf der Festplatte (Installation der optionalen Funktionen)
Anwendungsdefinitionstool	• Identisch mit Password Manager Agent	• Identisch mit Password Manager Agent

Hinweis: Password Manager wird nicht unter Microsoft Windows XP Home Edition unterstützt.

Hotdesktop wird nur unter Microsoft Windows 2000 Professional, Microsoft Windows XP Embedded und Microsoft Windows XP Professional, Service Pack 2 (32 Bit) unterstützt. Die Funktion wird nicht unter 64-Bit-Betriebssystemen oder Serverbetriebssystemen unterstützt.

Anforderungen für den Password Manager-Dienst

In dieser Tabelle sind die Hardware- und Softwareanforderungen für den Password Manager-Dienst aufgeführt.

Wichtig: Der Server mit dem Password Manager-Dienst enthält sehr vertrauliche Benutzerdaten. Sie sollten einen dedizierten Server verwenden, der an einem physisch sicheren Standort installiert ist.

Für die Softwaremodule des Password Manager-Dienstes gelten ebenfalls spezielle Konto- und Sicherheitsanforderungen. Weitere Informationen finden Sie unter „Sicherheits- und Kontoanforderungen für den Password Manager-Dienst“ auf Seite 81.

Password Manager-Komponenten	Unterstützte Umgebung bzw. unterstütztes Microsoft Windows-Betriebssystem mit dem aktuellen Service Pack	Hardware-anforderungen
Dienst	• Microsoft Windows Server 2003 mit Service Pack 2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit) • Microsoft Windows Server 2003, R2 (Standard Edition, Enterprise Edition, Datacenter Edition) (32 Bit) • ASP.NET (Anwendungsserverkomponenten verfügbar)	• 128 MB RAM • 30 Speicher-platz auf der Festplatte

ASP.NET-Anforderungen

Stellen Sie sicher, dass die Windows-Komponente ASP.NET auf dem Computer mit Windows Server 2003 installiert ist.

1. Öffnen Sie die Systemsteuerung und klicken Sie auf **Software**.
2. Klicken Sie auf **Windows-Komponenten hinzufügen/entfernen** und wählen Sie **Anwendungsserver**.
3. Klicken Sie auf **Details** und überprüfen Sie, ob ASP.NET installiert ist.

   Wenn das Kontrollkästchen für ASP.NET aktiviert ist, ist die Komponente installiert.

   Wenn das Kontrollkästchen für ASP.NET nicht aktiviert ist, ist die Komponente nicht installiert.
4. Wenn ASP.NET nicht installiert ist, aktivieren Sie das Kontrollkästchen. Klicken Sie dann auf **Weiter**. Klicken Sie nach Abschluss der Installation auf **Fertig stellen**.

Sicherheits- und Kontoanforderungen für den Password Manager-Dienst

Stellen Sie vor der Installation des Password Manager-Dienstes sicher, dass die entsprechenden Konten und Komponenten für die Unterstützung des Dienstes verfügbar sind. Da der Dienst HTTP (HTTPS) verwendet, wird ein Serverauthentifizierungszertifikat für die Kommunikation per SSL (Secure Sockets Layer) mit der Konsole und der Agentsoftware benötigt.

Anforderungen für das Serverauthentifizierungszertifikat

Hinweis: Bei der Installation des Password Manager-Dienstes werden Signatur- und Prüfungszertifikate erstellt, mit denen die Informationen im zentralen Speicher authentifiziert werden. Diese Zertifikate gehören nicht zum erforderlichen SSL-Zertifikat.

Besorgen Sie sich vor dem Installieren des Dienstes ein Serverauthentifizierungszertifikat zur SSL-Kommunikation bei einer Zertifizierungsstelle (CA) oder downloaden Sie Ihr persönliches Zertifikat auf den Server, wenn Sie eine vorhandene PKI (Public Key Infrastructure) verwenden.

Mit dem SSL-Zertifikat können Sie sicherstellen, dass die Datenübertragung vom Dienst zur Konsole und zur Agentsoftware sicher ist, und dass die Agentsoftware und Konsole mit dem richtigen Dienstserver kommunizieren.

- Da dieses Zertifikat zur SSL-Kommunikation verwendet wird, muss der allgemeine Name des Zertifikats mit dem vollqualifizierten Domänennamen des Dienstservers (FQDN) übereinstimmen. Geben Sie eine Mindestschlüssellänge von 1024 an.
- Sie müssen das Zertifikat im Zertifikatspeicher des lokalen Computers installieren und die entsprechenden Vertrauensstellungen für Konsole und Agent erstellen.
- Sie müssen dieses Zertifikat auf den Arbeitsstationen für den Dienst, die Konsole und den Agent installieren.

- In einer Umgebung mit Lastausgleich und Clusterdienst können Sie ein Zertifikat für mehrere Dienstserver verwenden, wenn der allgemeine Name des SSL-Zertifikats ein Platzhalterzeichen (in der Regel ein Sternchen) enthält. Verwenden Sie beispielsweise für eine Umgebung, die Server mit den Namen server1.mycompany.com, server2.mycompany.com und server3.mycompany.com umfasst, ein SSL-Zertifikat mit dem allgemeinen Namen server*.mycompany.com. Sie können in diesem Fall auch ein SSL-Zertifikat mit dem allgemeinen Namen *.mycompany.com verwenden, wobei der allgemeine Name nicht mit dem vollqualifizierten Domänennamen (FQDN) übereinstimmt. Weitere Informationen zur Konfiguration dieses Szenarios finden Sie unter „So konfigurieren Sie die Password Manager-Dienste“ auf Seite 108.

Wichtig: Wenn Sie das Zertifikat von einer Zertifizierungsstelle beziehen, die standardmäßig als nicht vertrauenswürdig gilt (z. B. eine in Ihrem Unternehmen installierte Zertifizierungsstelle), müssen Sie das Stammzertifikat im vertrauenswürdigen Stammzertifikatspeicher des lokalen Computers installieren, um die Vertrauensstellung herzustellen.

Wenn Sie SSL-Fehler feststellen, wird das Serverzertifikat wahrscheinlich nicht als vertrauenswürdig angesehen. Anweisungen zum Extrahieren und Bereitstellen von Stammzertifikaten einer Zertifizierungsstelle finden Sie auf der Website von Microsoft unter http://www.microsoft.com.

Erforderliche Konten für Dienstmodule

Für den Password Manager-Dienst können in der Umgebung bis zu drei verschiedene Systemkontotypen zum Lesen und Schreiben von Daten erforderlich sein.

- Dienstkonto
- Konto für Datenproxy
- Self-Service-Konto

Die Anzahl und der Typ der benötigten Konten hängt von den verwendeten Dienstmodulen ab. In der Tabelle sind die Konten aufgeführt, die Sie für jedes Dienstmodul benötigen. Wenn für unterschiedliche Module derselbe Kontotyp benötigt wird, können Sie dasselbe Konto für mehrere Module verwenden bzw. für jedes Modul eigene benutzerdefinierte Konten angeben.

Modul	**Benötigte Konten**		
	Dienst	**Datenproxy**	**Self-Service**
Datenintegrität	Ja	Nein	Nein
Schlüsselverwaltung	Ja	Ja	Nein
Provisioning	Ja	Ja	Nein
Self-Service	Ja	Ja	Ja
Synchronisierung der Anmeldeinfo	Ja	Nein	Nein

Anforderungen für Dienstkonten

Verwenden Sie auf dem Server, auf dem der Password Manager-Dienst ausgeführt wird, folgende Konten für den Dienst.

Betriebssystem	Kontoangabe
Windows 2003 Server	Verwenden Sie das vorhandene Konto **Netzwerkdienst** oder **Lokaler Dienst**.

Hinweis: Wenn Sie ein Domänenkonto als Dienstkonto erstellen, müssen Sie mit dem Dienstprogramm setspn.exe einen Dienstprinzipalnamen für dieses Domänenkonto und den Dienstserver in Active Directory registrieren. Weitere Informationen zu Dienstprinzipalnamen finden Sie auf der Website von Microsoft.

In dieser Version von Password Manager können lokale Benutzerkonten nicht als Dienstkonto definiert werden. Sie können das integrierte Konto **Lokaler Dienst** angeben.

Anforderungen für Datenproxykonten

Erstellen Sie auf dem Server mit dem Password Manager-Dienst ein Konto mit den folgenden Einstellungen und verwenden Sie es für die Datenproxykommunikation mit dem Dienst.

Das Konto muss Lese- und Schreibzugriff auf den zentralen Speicher haben. Die Kontoanforderungen hängen vom Typ des zentralen Speichers ab, der implementiert wird.

Typ des zentralen Speichers	Kontobeschreibung
NTFS-Netzwerkfreigabe	Für das Konto gilt: • Konto benötigt Lese- und Schreibzugriff auf den zentralen Speicher • Konto ist Mitglied einer Domäne Gehen Sie nach dem Erstellen des zentralen Speichers wie folgt vor: • Erteilen Sie dem Konto die Berechtigung **Volle Kontrolle** für die Freigabe **CITRIXSYNC$**. • Erteilen Sie dem Konto die Berechtigung **Volle Kontrolle** für den Ordner **CITRIXSYNC** und dessen Unterordner: Ordner **CentralStoreRoot** und Ordner **People** • Erteilen Sie dem Konto die Berechtigung **Volle Kontrolle** für alle Dateiobjekte im Ordner **CITRIXSYNC** und dessen Unterordner: • Stellen Sie sicher, dass die Gruppe **Authentifizierte Benutzer** Ordner im Ordner **People** erstellen kann.
Active Directory	Das Konto muss die folgenden Bedingungen erfüllen: • Konto benötigt Lese- und Schreibzugriff auf den zentralen Speicher • Es ist Mitglied der Gruppe **Domänenadministratoren**.

Hinweis: Der Password Manager-Dienst kann nicht verwendet werden, wenn der zentrale Speicher ein freigegebener Novell Ordner ist.

Self-Service-Anforderungen

Wenn Sie die Funktionen des Moduls **Konto-Self-Service** zur benutzerseitigen Kennwortzurücksetzung bzw. Aufhebung der Kontosperrung verwenden, benötigen Sie ein Konto, das Mitglied der Gruppe **Domänenadministratoren** ist.

Kontoanforderungen zum Installieren und Verwenden von Password Manager

Im folgenden Abschnitt werden die Kontoanforderungen für Benutzer beschrieben, die Komponenten von Password Manager installieren und verwenden.

- Installieren und Verwenden des Password Manager-Dienstes
- Installieren und Verwenden der Password Manager Console und des Anwendungsdefinitionstools
- Installieren und Verwenden von Password Manager Agent

Installieren und Verwenden des Password Manager-Dienstes

Der Benutzer, der den Dienst installiert und den Assistenten für die Dienstkonfiguration ausführt, muss ein Mitglied der Domäne (ein Domänenbenutzer) sowie ein Mitglied der lokalen Gruppe **Administratoren** auf dem Dienstcomputer sein. (Fügen Sie der lokalen Gruppe **Administratoren** ein Domänenbenutzerkonto hinzu.) Das Domänenbenutzerkonto muss kein Domänenadministrator sein.

Installieren und Verwenden der Password Manager Console und des Anwendungsdefinitionstools

Der Benutzer, der die Konsole installiert, eine Discovery in der Konsole ausführt, die Konsole konfiguriert und später verwendet, muss ein Domänenadministrator und Mitglied der lokalen Gruppe **Administratoren** auf der Arbeitsstation der Konsole sein. Für dieses Benutzerkonto ist Lese- und Schreibzugriff auf den zentralen Speicher erforderlich. Ein Benutzerkonto ohne Administratorrechte kann die Verwaltungsrechte für die Konsole und die zugehörigen Funktionen über eine Delegierung bzw. begrenzte Delegierung mit Active Directory erhalten.

Installieren und Verwenden von Password Manager Agent

Der Benutzer, der die Agentsoftware installiert, muss ein Mitglied der Domäne (ein Domänenbenutzer) sowie ein Mitglied der lokalen Gruppe **Administratoren** auf dem Dienstcomputer sein. Das Domänenbenutzerkonto muss kein Domänenadministrator sein.

Der Benutzer, der die Agentsoftware ausführt, muss ein Mitglied der Domäne (ein Domänenbenutzer) sein.

Installieren von Microsoft .NET 2.0 Framework

In diesem Abschnitt wird die Installation von Microsoft .NET 2.0 Framework von der Password Manager-CD beschrieben. Sie müssen diese Rahmenanwendung auf jedem Computer in der Umgebung installieren, auf dem Folgendes installiert wird:

- Konsole
- Dienst
- Anwendungsdefinitionstool

Wichtig: Die für die Installation von Password Manager erforderliche Version von .NET 2.0 Framework ist auf der Password Manager-CD enthalten. Verwenden Sie diese Version oder .NET 3.0.

Lesen Sie immer die Datei readme.htm file auf der Citrix Website (http://www.citrix.com) für Updates und aktuelle Informationen. (Öffnen Sie die Datei Password_Manager_Read_Me_First.html im Ordner \Documentation auf der CD, um auf die Readmedatei und andere Password Manager-Dokumentation zuzugreifen.)

„Side-by-Side“-Installation von .NET 2.0 und .NET 1.1

Auf einer Arbeitsstation oder einem Server mit .NET 1.1 kann .NET 2.0 zusätzlich installiert werden. Dies wird als *Side-by-Side*-Installation bezeichnet. Sie müssen .NET 1.1 auf keinem Computer deinstallieren, auf dem Sie die folgenden Funktionen von Password Manager installieren möchten:

- Konsole
- Dienst
- Anwendungsdefinitionstool

Hinweis: Weitere Informationen zum Vorgehen bei einem Upgrade der Konsolensoftware finden Sie unter „Microsoft .NET Version 1.1 und 2.0“ auf Seite 140.

So installieren Sie Microsoft .NET 2.0

1. Legen Sie die CD in das CD-ROM-Laufwerk des Computers ein, auf dem Sie die Konsole, den Dienst oder das Anwendungsdefinitionstool installieren möchten.
2. Führen Sie einen der folgenden Schritte aus:
   - Bei aktivierter Autorun-Funktion wird der Installationsbildschirm von Citrix Password Manager angezeigt. Klicken Sie auf **CD durchsuchen**, um Windows Explorer zu öffnen.
   - Bei deaktivierter Autorun-Funktion öffnen Sie Windows Explorer und rufen Sie das CD-ROM-Laufwerk auf.
3. Öffnen Sie den Ordner **Support** und anschließend den Ordner **DotNet20**.
4. Führen Sie einen der folgenden Schritte aus:
   - Für 32-Bit-Systeme öffnen Sie den Ordner x86 und klicken Sie dann auf die Datei dotnetfx.exe
   - Für 64-Bit-Systeme öffnen Sie den Ordner x64 und klicken Sie dann auf die Datei dotnet.exe
5. Klicken Sie im Sicherheitshinweisfenster auf **Ausführen**.
6. Durchlaufen Sie die einzelnen Installationsfenster, um .NET 2.0 Framework zu installieren.
7. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.

Hinweis: Bei nicht-englischen Betriebssystemen können Sie das Microsoft .NET Framework Version 2.0 Sprachpaket installieren, um die .NET Framework-Sprachunterstützung einzurichten. Es steht auf der Microsoft Website (http://www.microsoft.com) zur Verfügung.

Installieren von Java Runtime Environment

Password Manager unterstützt die JRE Versionen 1.4.x, 1.5.x (wird auch 5.0 genannt) und 1.6.x (6.0). JRE Version 1.5, Update 9, finden Sie auf der Produkt-CD im Unterordner \Support\JRE15009. Sie können auch die aktuell unterstützte Version von der Sun Microsystems Website (http://java.sun.com) herunterladen.

Sie können JRE auf Computern bei der Installation folgender Komponenten installieren:

- Konsole
- Anwendungsdefinitionstool
- Agentsoftware

Installieren oder Aktualisieren von JRE nach der Installation der Konsole, des Anwendungsdefinitionstools oder der Agentsoftware

Aktualisieren Sie über die Systemsteuerung die auf dem Computer installierte Password Manager-Software, wenn Sie JRE nach der Installation der Konsole, des Anwendungsdefinitionstools oder der Agentsoftware installieren oder aktualisieren. Dadurch wird die aktuelle JRE-Version diesen Password Manager-Komponenten zugeordnet. Siehe auch „Problembehandlung bei Java-bezogenen Fehlermeldungen beim Installieren oder Deinstallieren der Agentsoftware“ auf Seite 91.

So ordnen Sie JRE der Password Manager-Anwendung zu

1. Klicken Sie auf **Start > Einstellungen > Systemsteuerung**.
2. Klicken Sie auf **Software**.
3. Wählen Sie eine der folgenden Optionen aus und klicken Sie auf **Ändern**:
   - **Citrix Password Manager Console**
   - **Citrix Password Manager Agent**
   - **Citrix Password Manager-Anwendungsdefinitionstool**
4. Wählen Sie im Setup-Dialogfeld die Option **Reparieren** und klicken Sie zweimal auf **Weiter**.
5. Klicken Sie nach dem erfolgreichen Reparieren der Konsole auf **Fertig stellen**.

Problembehandlung bei Java-bezogenen Fehlermeldungen beim Installieren oder Deinstallieren der Agentsoftware

Unter Umständen wird beim Installieren bzw. Deinstallieren der Agentsoftware die folgende Fehlermeldung angezeigt:

```
Citrix Password Manager hat erkannt, dass mehrere Java-
Softwareprogramme oder Dateien aktuell verwendet werden.  Schließen
Sie alle Programme und halten Sie alle Java-bezogenen Dienste an,
bevor Sie den Vorgang fortsetzen.
```

Dieser Fehler tritt meist dann auf, wenn Sie die Agentsoftware auf einem PC installieren, auf dem auch ein Webserverdienst (z. B. Apache Tomcat, Apache HTTP-Server usw.) ausgeführt wird. Die Fehlermeldung kann auch angezeigt werden, wenn Sie die Agentsoftware auf einem Computer mit Citrix Presentation Server mit installierter License Management Console installieren.

Gehen Sie in diesem Fall wie folgt vor:

1. Beenden Sie den Dienst.
2. Installieren bzw. deinstallieren Sie die Agentsoftware.
3. Starten Sie den Dienst neu.

Lizenzierungsanforderungen

Citrix empfiehlt, dass Sie zuerst den Lizenzserver installieren und die Lizenzen hinzufügen, bevor Sie Password Manager installieren.

Weitere Informationen zu den Lizenzierungsanforderungen, Bedingungen und zur Installation finden Sie im Handbuch *Schnelleinstieg für die Citrix Lizenzierung*, das auf der Website http://support.citrix.com/licensing/ unter dem Seitentitel „Top Licensing Resources“ zur Verfügung steht. Informationen zur Verwendung von Lizenzen benannter und gleichzeitiger Benutzer in Password Manager finden Sie im *Citrix Password Manager-Administratorhandbuch*.

Hinweis: Öffnen Sie die Datei Password_Manager_Read_Me_First.html im Ordner \Documentation auf der CD, um auf das Handbuch *Schnelleinstieg für die Citrix Lizenzierung*, *Citrix Password Manager-Administratorhandbuch* und andere Password Manager-Dokumentation zuzugreifen. Sie finden weitere Lizenzierungsressourcen unter http://support.citrix.com/licensing/ unter dem Seitentitel „Top Licensing Resources“.

Vor der Installation von Password Manager

Hinweis: Weitere Informationen finden Sie unter „Kontoanforderungen zum Installieren und Verwenden von Password Manager“ auf Seite 86.

Mit Autorun können Sie verschiedene Password Manager-Aufgaben ausführen, zum Beispiel einen zentralen Speicher erstellen oder Komponenten von Password Manager installieren. Wenn Sie die Produkt-CD in das CD-ROM-Laufwerk eingelegt haben, wird Autorun-Installationsbildschirm angezeigt.

Wenn dieses Dialogfeld nicht automatisch angezeigt wird, gehen Sie wie folgt vor:

1. Öffnen Sie Windows Explorer und wählen Sie das CD-ROM-Laufwerk aus.
2. Klicken Sie auf Autorun.exe.

Installationsreihenfolge

Es wird empfohlen, Password Manager in der folgenden Reihenfolge zu installieren:

- Lizenzieren Sie Password Manager. (Weitere Informationen finden Sie unter „Lizenzierungsanforderungen“ auf Seite 92.)
- Erstellen Sie den zentralen Speicher.
- Installieren Sie den Password Manager-Dienst, wenn Sie mindestens eines der folgenden Module verwenden möchten:
  - Schlüsselverwaltung
  - Self-Service
  - Provisioning
  - Synchronisierung der Anmeldeinformationen
  - Datenintegrität

  Hinweis: Wenn Sie das Modul **Datenintegrität** zu einem späteren Zeitpunkt installieren möchten oder die Konsole und die Agentsoftware installiert haben, müssen Sie die vorhandenen Daten im zentralen Speicher mit dem Datensignierungstool CtxSignData.exe digital signieren. (Dieses Tool steht nach der Installation des Moduls Datenintegrität zur Verfügung.) Umgekehrt müssen Sie die Signierung der Daten im zentralen Speicher aufheben, wenn Sie das Modul **Datenintegrität** deinstallieren. Weitere Informationen zur Signatur von Daten finden Sie unter „Aktivieren und Deaktivieren des Datenintegritätsdienstes in der Password Manager Agent-Software“ im *Citrix Password Manager-Administratorhandbuch*.
- Installieren Sie die Password Manager Console auf den Computern in der Umgebung.
- Wenn Sie nur Anwendungsdefinitionen erstellen möchten, installieren Sie das Anwendungsdefinitionstool auf den Computern in der Umgebung.
- Wenn Sie die Password Manager-Funktionen in der Konsole konfiguriert haben, installieren Sie Password Manager Agent auf allen Benutzercomputern in der Umgebung. Sie können die Agentsoftware auch als veröffentlichte Anwendung in einer Citrix Presentation Server-Umgebung bereitstellen.

Installationsort der einzelnen Komponenten von Password Manager

Wichtig: Installieren Sie den Dienst und Agent nicht auf demselben Computer.

Installieren Sie Password Manager nicht auf Domänencontrollern. Das Installieren einer Komponente von Password Manager (Agent, Dienst, Konsole oder zentraler Speicher) auf einem Domänencontroller wird nicht unterstützt.

Weitere Informationen finden Sie auch unter „Kontoanforderungen zum Installieren und Verwenden von Password Manager“ auf Seite 86.

Folgende Kombinationen oder Szenarios sind für die Installation des Dienstes, der Konsole und der Agentsoftware zulässig:

- Installieren Sie den Dienst und die Konsole auf demselben Computer.
- Installieren Sie die Konsole und den Agent auf demselben Computer.
- Installieren Sie den Agent auf einem beliebigen Computer oder Clientgerät in der Umgebung, um den Zugriff auf lokal installierte Single Sign-On-aktivierte Anwendungen zu ermöglichen.
- Installieren Sie die Konsole und das Anwendungsdefinitionstool auf einem Computer in der Umgebung.
- Zu Testzwecken können Sie auch die Konsole und den Agent auf demselben Computer installieren, um sicherzustellen, dass Änderungen an der Konsole vom Agent übernommen werden.
- Stellen Sie die Agentsoftware in einer Citrix Presentation Server-Umgebung bereit. In diesem Fall werden vom Agent nur Anmelde-informationen für Anwendungen gesendet oder bereitgestellt, die in Presentation Server veröffentlicht wurden (und nicht für Anwendungen, die lokal auf der Arbeitsstation des Benutzers oder dem Clientgerät installiert wurden).

Wichtig: Der Server mit dem Password Manager-Dienst und zentralen Speicher enthält sehr vertrauliche Benutzerdaten. Sie sollten einen dedizierten Server verwenden, der an einem physisch sicheren Standort installiert ist.

Erstellen eines zentralen Speichers

Bei den folgenden Schritten wird davon ausgegangen, dass die Password Manager-CD in den Computer eingelegt ist, der als Host für den zentralen Speicher dient, und dass der Autorun-Bildschirm angezeigt wird.

Lesen Sie vor dem Erstellen des zentralen Speichers die folgenden Themen:

- Planen der Password Manager-Umgebung, „Auswählen des Typs des zentralen Speichers“ auf Seite 23
- „Verwenden der Kontozuordnung mit mehreren zentralen Speichern und Kontoanmeldeinformationen der Benutzer in einem Unternehmen mit mehreren Domänen“ auf Seite 30
- „Vor der Installation von Password Manager“ auf Seite 93

Hinweis: Wenn Sie benutzerdefinierte Parameter für den zentralen Speicher festlegen möchten, können Sie ihn auch an einer Befehlszeile erstellen. Siehe „Erstellen eines zentralen Speichers an einer Befehlszeile (optional)“ auf Seite 99.

So erstellen Sie einen zentralen Speicher auf einer NTFS-Netzwerkfreigabe

1. Klicken Sie auf **Schritt 2: Zentralen Speicher erstellen**.
2. Klicken Sie auf **Zentralen Speicher auf einer NTFS-Netzwerkfreigabe erstellen**.
3. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

   Ein Befehlsfenster wird angezeigt.
4. Drücken Sie nach dem Erstellen des zentralen Speichers eine beliebige Taste, um das Befehlsfenster zu schließen.

Unter C:\CITRIXSYNC wurde nun ein NTFS-Netzwerkfreigabeordner erstellt.

Hinweis: Wenn Benutzer, die keine Administratoren auf den Dateiservern sind, die Password Manager-Ordner verwalten müssen, können Sie die Benutzer dem freigegebenen Stammordner mit vollständigen Rechten hinzufügen. Sie müssen diese Benutzer auch dem Ordner People und dem Ordner CentralStoreRoot hinzufügen, da diese Ordner nicht die Zugriffsrechte vom freigegebenen Stammordner übernehmen.

Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.

So erstellen Sie einen zentralen Speicher in einem freigegebenen Novell Ordner

Hinweis: Stellen Sie sicher, dass Sie den zentralen Speicher auf einem Computer erstellen, auf dem der Novell Client installiert ist.

Berücksichtigen Sie außerdem, dass die Agentsoftware, die auf 64-Bit-Computern ausgeführt wird, keine Verbindung zu zentralen Speichern in freigegebenen Novell Ordnern herstellen kann.

1. Klicken Sie auf **Schritt 2: Zentralen Speicher erstellen**.
2. Klicken Sie auf **Zentralen Speicher in einem freigegebenen Novell Ordner erstellen**.
3. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

   Ein Befehlsfenster wird angezeigt.
4. Geben Sie an der Eingabeaufforderung PATH: einen UNC-Pfad zum NetWare-Server, Volume und Ordner an, die Sie erstellen möchten.

   Beispiel: **\\NW5SRV\DATA\CITRIXSYNC$**.
5. Drücken Sie nach dem Erstellen des zentralen Speichers eine beliebige Taste, um das Windows-Befehlsfenster zu schließen.

Jetzt wurde ein freigegebener Novell Ordner erstellt.

So erstellen Sie einen zentralen Speicher unter Active Directory

Hinweis: Stellen Sie sicher, dass der aktuelle Server zur Active Directory-Domäne gehört und der aktuelle Benutzer ein Mitglied der Gruppe **Schemaadministratoren** und der Gruppe **Domänenadministratoren** ist. Stellen Sie sicher, dass der Active Directory-Schemamaster so konfiguriert ist, dass Updates zulässig sind.

1. Klicken Sie auf **Schritt 2: Zentralen Speicher erstellen**.
2. Klicken Sie auf **Zentralen Speicher in Active Directory-Domäne erstellen**.
3. Klicken Sie auf **Schritt 1: Active Directory-Schema erweitern**.
4. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

   Ein Befehlsfenster wird angezeigt.
5. Drücken Sie nach dem Erstellen des Schemas eine beliebige Taste, um das Befehlsfenster zu schließen.

   Hinweis: Stellen Sie vor dem Ausführen des nächsten Schritts sicher, dass die Schemaerweiterung von allen Domänencontrollen in der Active Directory-Umgebung übernommen wurde.
6. Klicken Sie auf **Schritt 2: Zentralen Speicher im erweiterten Schema erstellen**.
7. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

   Ein Befehlsfenster wird angezeigt.
8. Drücken Sie nach dem Erstellen des Schemas eine beliebige Taste, um das Befehlsfenster zu schließen.

Jetzt wurde der zentrale Speicher unter Active Directory erstellt. Weitere Informationen finden Sie auch unter „Auswählen von Active Directory als zentralen Speicher“ auf Seite 25.

Erstellen eines zentralen Speichers an einer Befehlszeile (optional)

Bei der Installation von Password Manager können Sie einen zentralen Speicher auch an einer Befehlszeile in einem Eingabeaufforderungsfenster erstellen. Beim Erstellen eines zentralen Speichers an der Befehlszeile können Sie statt der Standardparameter im Installationsfenster von Password Manager benutzerdefinierte Parameter verwenden.

In dieser Tabelle sind die Typen für den zentralen Speicher und die zugeordneten Dienstprogramme aufgeführt. Diese Dienstprogramme befinden sich im Ordner \Tools auf der Password Manager-CD.

Dienstprogramm	Dateiname	Zweck und Beschreibung
Dienstprogramm zur Schemaerweiterung in Active Directory	CtxSchemaPrep.exe	Zum Erstellen eines zentralen Speichers unter Active Directory. Erweitert das Active Directory-Schema für die Verwendung mit Password Manager.
Dienstprogramm zur Domänenvorbereitung in Active Directory	CtxDomainPrep.exe	Zum Erstellen eines zentralen Speichers unter Active Directory. Aktualisiert die Berechtigungen des Active Directory-Domänenstamms, damit Benutzer Password Manager-Objekte unter dem Benutzerobjekt erstellen können.
Dienstprogramm zum Dateisynchronisierungssetup	CtxFileSyncPrep.exe	Zum Erstellen eines zentralen Speichers auf einer NTFS-Netzwerkfreigabe.
Dienstprogramm zum Dateisynchronisierungssetup für Novell NetWare	CtxNWFileSyncPrep.exe	Zum Erstellen eines zentralen Speichers in einem öffentlich zugänglichen freigegebenen Novell Ordner.

Weitere Informationen finden Sie unter:

- „Erstellen eines zentralen Speichers unter Active Directory“ auf Seite 100
- „Erstellen eines zentralen Speichers auf einer NTFS-Netzwerkfreigabe“ auf Seite 102
- „Erstellen eines zentralen Speichers in einem freigegebenen Novell Ordner“ auf Seite 104

Erstellen eines zentralen Speichers unter Active Directory

Das Erstellen eines zentralen Speichers unter Active Directory erfolgt in zwei Schritten:

- Erweitern Sie Ihr Active Directory-Schema für eine Verwendung mit Password Manager.
- Aktualisieren Sie die Berechtigungen des Active Directory-Domänenstamms, damit Benutzer Password Manager-Objekte unter dem Benutzerobjekt erstellen können.

Hinweis: Stellen Sie sicher, dass der Active Directory-Schemamaster so konfiguriert ist, dass Updates zulässig sind.

So erstellen Sie den zentralen Speicher automatisch von einer Befehlszeile aus - Schritt 1: Erweitern Sie das Active Directory-Schema

1. Melden Sie sich mit einem Konto mit Anmeldeinformationen der Gruppe **Schemaadministratoren** an einem Server in der Active Directory-Domäne an.
2. Stellen Sie sicher, dass der Computer mit der Rolle des Schemamasters so konfiguriert ist, dass Schemaaktualisierungen erlaubt sind.
3. Greifen Sie an der Eingabeaufforderung auf das Verzeichnis \Tools auf der Produkt-CD zu.
4. Geben Sie **CtxSchemaPrep.exe** ein.
5. Stellen Sie sicher, dass alle Schemaänderungen auf allen Domänencontrollern im Unternehmen bereitgestellt wurden, bevor Sie fortfahren.

So erstellen Sie den zentralen Speicher automatisch von einer Befehlszeile aus - Schritt 2: Aktualisieren Sie die Berechtigungen für den Domänenstamm

1. Bevor Sie fortfahren, sollten Sie sicherstellen, dass die in Schritt 1 ausgeführten Schemaänderungen von allen Domänencontrollern im Unternehmen übernommen wurden.
2. Melden Sie sich mit einem Konto mit Anmeldeinformationen der Gruppe **Domänenadministratoren** an einem Computer an, der sich in der Domäne befindet, die Sie konfigurieren möchten.
3. Greifen Sie an der Eingabeaufforderung auf das Verzeichnis \Tools auf der Produkt-CD zu.
4. Geben Sie **CtxDomainPrep.exe** [*Distinguished Name*] ein.

   Wobei Folgendes gilt:

Distinguished Name	Relativer DN (Distinguished Name) der Organisationseinheit (OU), für die die Berechtigungen festgelegt werden. Dieser DN wird an den DN des Domänenstamms angehängt. Mit dieser Option können Sie eine Organisationseinheit angeben, um Berechtigungen auf der Ebene der Organisationseinheit statt auf der Ebene des Domänenstamms festzulegen. Diese Methode beschränkt die Verwendung von Password Manager auf die angegebene Organisationseinheit. Beispiel: `CtxDomainPrep.exe OU=Employees` Die Berechtigungen werden auf OE=Mitarbeiter, DC=Ihre Domäne, DC=com festgelegt.

5. Folgen Sie den Anweisungen auf dem Bildschirm, um das Erstellen des zentralen Speichers abzuschließen.

Erstellen eines zentralen Speichers auf einer NTFS-Netzwerkfreigabe

Das Setupprogramm zur NTFS-Dateisynchronisierung CtxFileSyncPrep.exe erstellt automatisch die erforderlichen Ordner für den zentralen Speicher. Außerdem werden der freigegebene Ordner, der Ordner CentralStoreRoot und der Ordner People mit den erforderlichen Freigabe- und Sicherheitsberechtigungen erstellt.

Dabei müssen Sie Folgendes sicherstellen:

- Der zentrale Speicher muss zu derselben Domäne wie die Computer mit Presentation Server oder die Arbeitsstationen gehören, auf denen die Agentsoftware installiert ist.
- Führen Sie CtxFileSyncPrep.exe auf dem Server aus, auf dem die NTFS-Netzwerkfreigabe gehostet wird.

Hinweis: Wenn Benutzer, die keine Administratoren auf den Dateiservern sind, die Password Manager-Ordner verwalten müssen, können Sie die Benutzer dem freigegebenen Stammordner mit vollständigen Rechten hinzufügen. Sie müssen diese Benutzer auch dem Ordner People und dem Ordner CentralStoreRoot hinzufügen, da diese Ordner nicht die Zugriffsrechte vom freigegebenen Stammordner übernehmen. Geben Sie diesen Benutzern volle Berechtigungen zur Freigabe von Berechtigungen, Dateien und Unterordnern im Ordner **People** und **CentralStoreRoot**.

Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.

So erstellen Sie einen zentralen Speicher auf einer NTFS-Netzwerkfreigabe automatisch an einer Befehlszeile

1. Greifen Sie auf dem Server, der die NTFS-Netzwerkfreigabe hostet, von einer Eingabeaufforderung aus auf das Verzeichnis \Tools auf der Produkt-CD zu.
2. Geben Sie **CtxFileSyncPrep** [**/path:***Pfadname*] [**/share:***Freigabename*] [**/Admin:**[+|-]*Kontoname*] ein.

   Wobei Folgendes gilt:

/path:*Pfadname*	Gibt den Pfadnamen für die NTFS-Netzwerkfreigabe auf dem lokalen Server an. Wenn Sie diesen Parameter verwenden, muss sich der Pfadname auf dem lokalen Server befinden. Wenn Sie /path:*Pfadname* nicht festlegen, wird der zentrale Speicher mit diesem Befehl unter %SystemDrive%\CITRIXSYNC erstellt.
/share:*Freigabename*	Gibt den Freigabenamen für die NTFS-Netzwerkfreigabe auf dem lokalen Server an. Wenn Sie /share:*Freigabename* nicht festlegen, wird der Freigabeparameter für den zentralen Speicher mit diesem Befehl unter CITRIXSYNC$ erstellt.
/Admin:[+|-]*Kontoname*	Hinzufügen oder Entfernene eines Kontonamens, damit das Konto einen freigegebenen Ordner verwalten kann. Wenn Sie das Plus- oder Minuszeichen nicht angeben, ist das Pluszeichen der Standardoperator zum Hinzufügen eines Kontos. Fügen Sie mit dem Pluszeichen (+) ein Konto hinzu, wobei der Kontoname als Domänenname\Benutzername oder Benutzername@Domäne eingegeben wird. Mit dem Minuszeichen (-) entfernen Sie das Konto oder deaktivieren die Administratorrechte.

Die Ordner **CentralStoreRoot** und **People** werden mit den entsprechenden Freigabe- und Sicherheitsberechtigungen erstellt. Der freigegebene Ordner kann nun für die Synchronisierung verwendet werden.

Erstellen eines zentralen Speichers in einem freigegebenen Novell Ordner

Das Setupprogramm für den freigegebenen Novell Ordner CtxNWFileSyncPrep.exe erstellt automatisch die erforderlichen Ordner für den zentralen Speicher. Außerdem werden der freigegebene Ordner, der Ordner CentralStoreRoot und der Ordner People mit den erforderlichen Freigabe- und Sicherheitsberechtigungen erstellt.

Überlegungen

- Da der Agent ein Windows-Kennwort verwendet, müssen bei der Verwendung der Novell Netware-Datensynchronisierung die Kennwörter der Benutzer für Novell und Windows identisch sein.
- Der zentrale Speicher muss in derselben Struktur sein wie die Computer, auf denen Instanzen der Agentsoftware installiert sind.
- Benutzer müssen sich an einer Novell-Struktur anmelden, die den freigegebenen Ordner enthält.
- Darüber hinaus benötigen die Benutzer auch Konten mit Leseberechtigung für den freigegebenen Ordner von Novell Netware, den Sie als zentralen Speicher angegeben haben.
- Alle Benutzer ohne Supervisor-Rechte, die Ordner im Rahmen von Password Manager verwalten müssen, können dem Synchronisierungs-Stammverzeichnis als Vertrauensnehmer mit vollständigen Rechten hinzugefügt werden. Dies verleiht ihnen die erforderlichen Zugriffsrechte für alle Ordner und Dateien, die dem Synchronisierungsordner untergeordnet sind.

Wichtig: Citrix rät davon ab, für das Hosten des freigegebenen Ordners den Systemdatenträger zu verwenden. Auf dem Systemdatenträger steht normalerweise nur ein begrenzter Speicherplatz zur Verfügung. Wenn Daten zum zentralen Speicher geschrieben werden, könnte der Systemdatenträger keinen freien Speicherplatz mehr haben, sodass die Password Manager-Umgebung (und möglicherweise der Novell NetWare-Server) nicht mehr funktionsfähig ist.

So erstellen Sie den zentralen Speicher in einem freigegebenen Novell Ordner automatisch an einer Befehlszeile

1. Greifen Sie auf dem Server, der den freigegebenen Novell Ordner hostet, von einer Eingabeaufforderung aus auf das Verzeichnis \Tools auf der Produkt-CD zu.
2. Geben Sie **CtxNWFileSyncPrep /path:\\NetWare-Server \Volume\Ordner [allowsysvol]** ein.

   Wobei Folgendes gilt:

/path:*NetWare-Server/ Volume/Ordner*	Erforderlicher Parameter, der den UNC-Pfad zum NetWare-Server, Volume und Ordner des zu erstellenden zentralen Speichers festlegt. Verwenden Sie keinen vorhandenen Ordner, da der Ordner vom Dienstprogramm erstellt wird. Beispiel: /path:\\NW5SRV\DATA\CITRIXSYNC

Die Ordner **CentralStoreRoot** und **People** werden jetzt mit den entsprechenden Freigabe- und Sicherheitsberechtigungen erstellt. Der freigegebene Ordner kann nun für die Synchronisierung verwendet werden.

Installieren und Konfigurieren des Password Manager-Dienstes

Die einzelnen Password Manager-Dienstmodule, die installiert werden können, werden unter „Auswählen optionaler Funktionen des Password Manager-Dienstes“ auf Seite 57 beschrieben. Nach der Installation des Dienstes wird der Assistent für die Dienstkonfiguration ausgeführt, mit dem Sie den Dienst konfigurieren und aktivieren können.

Berücksichtigen Sie bei der Installation und Konfiguration folgenden Ablauf:

- Erwerben und installieren Sie ein SSL-Zertifikat auf den Computern für Dienst, Konsole und Agent. Weitere Informationen finden Sie unter „Sicherheits- und Kontoanforderungen für den Password Manager-Dienst“ auf Seite 81.
- Erstellen Sie den erforderlichen Kontotyp für die zu installierenden Dienste. Weitere Informationen finden Sie unter „Erforderliche Konten für Dienstmodule“ auf Seite 83.
- Installieren Sie den Dienst bzw. die Dienste. Weitere Informationen finden Sie unter „Vor der Installation von Password Manager“ auf Seite 93.
- Schließen Sie den Assistenten für die Dienstkonfiguration ab.

Bei den folgenden Schritten wird davon ausgegangen, dass die Password Manager-CD in den Computer eingelegt ist, der als Host für den zentralen Speicher dient, und dass der Autorun-Bildschirm angezeigt wird.

So installieren Sie die Dienstmodule

1. Klicken Sie auf **Schritt 3: Administrative Komponenten installieren**.
2. Klicken Sie auf **Schritt 2: Password Manager-Dienst installieren (falls zutreffend)**.
3. Klicken Sie auf **Weiter**, stimmen Sie der Lizenzvereinbarung zu und klicken Sie erneut auf **Weiter**.
4. Wählen Sie im Dialogfeld **Module auswählen** die Module aus, die Sie installieren möchten:
   - Schlüsselverwaltung
   - Datenintegrität
   - Provisioning
   - Self-Service
   - Synchronisierung der Anmeldeinfo
5. Klicken Sie auf **Weiter**.

   Wenn Sie die ausgewählten Module ändern möchten, klicken Sie auf **Zurück**.
6. Klicken Sie auf **Installieren**.
7. Klicken Sie auf **Fertig stellen**.

Der Assistent für die Dienstkonfiguration wird gestartet.

So konfigurieren Sie die Password Manager-Dienste

Hinweis: Der Assistent für die Dienstkonfiguration wird gestartet, nachdem ein oder mehrere Dienstmodule erfolgreich installiert wurden. Nach der Erstkonfiguration können Sie den Assistenten jederzeit ausführen, indem Sie auf **Start > Programme > Citrix > Password Manager > Dienstkonfiguration** klicken.

Auf dem **Begrüßungsbildschirm** sind alle erkannten installierten Dienstmodule aufgeführt.

1. Klicken Sie auf dem Begrüßungsbildschirm der Dienstkonfiguration auf **Weiter**.
2. Geben Sie auf dem Bildschirm **Dienst konfigurieren** Folgendes an:

Verbindungseinstellung	Geben Sie die Portnummer für die Dienstverbindung an. Der Standardport ist 443. Weitere Informationen finden Sie unter „Portnummer für den Password Manager-Dienst“ auf Seite 112.
SSL-Zertifikat	Wählen Sie das auf dem Dienstcomputer installierte SSL-Zertifikat aus, das für die Kommunikation mit Clientcomputern verwendet wird. Aktivieren Sie das Kontrollkästchen **Ausführlichen Namen anzeigen**, um die im Zertifikat enthaltenen LDAP-Informationen anzuzeigen.
Name des virtuellen Hosts	Standardmäßig ist die Option **Standardwert verwenden** ausgewählt, wenn der Name des SSL-Zertifikats mit dem Namen des virtuellen Hosts übereinstimmt. Der Name des virtuellen Hosts muss mit dem Namen des SSL-Zertifikats übereinstimmen. Der virtuelle Host ist der Rechnername, der Benutzern beim Erstellen des Zertifikats angezeigt wurde. Dies muss nicht der tatsächliche Rechnername sein. Der Zertifikatsname kann beispielsweise ein Platzhalterzeichen (ein Sternchen) enthalten oder einen Domänennamen, dessen Groß- bzw. Kleinschreibung nicht mit dem Domänennamen des Zertifikats übereinstimmt. Diese Einstellung ist sinnvoll in Umgebungen mit Lastausgleich oder Clusterdienst. Weitere Informationen finden Sie unter „Sicherheits- und Kontoanforderungen für den Password Manager-Dienst“ auf Seite 81.
Kontoanmeldeinformationen	Wählen Sie das Konto des lokalen Computers aus, das für den Dienst verwendet wird. In der Regel können Sie das Konto **Netzwerkdienst** auswählen. Weitere Informationen finden Sie unter „Anforderungen für Dienstkonten“ auf Seite 84.

3. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Signaturzertifikat erstellen** wird angezeigt.

4. Führen Sie einen der folgenden Schritte aus:

   - Wenn der Assistent ein Signaturzertifikat erkennt, klicken Sie auf **Weiter**.
   - Wenn kein Signaturzertifikat vorhanden ist, geben Sie eine Gültigkeitsdauer (in Monaten) für das Signaturzertifikat ein. Die standardmäßige Gültigkeitsdauer beträgt 12 Monate. Klicken Sie auf **Weiter**.

   Die Seite **Datenproxy konfigurieren** wird angezeigt.

5. Führen Sie einen der folgenden Schritte aus:

   - Wenn Sie einen zentralen Speicher unter Active Directory erstellt haben, wählen Sie **Active Directory** und klicken Sie auf **Weiter**.
   - Wenn Sie einen zentralen Speicher auf einer NTFS-Netzwerkfreigabe erstellt haben, wählen Sie **NTFS-Netzwerkfreigabe**, geben Sie den UNC-Pfad zum zentralen Speicher ein, die Sie unter „Erstellen eines zentralen Speichers“ auf Seite 96 erstellt haben, und klicken Sie auf **Weiter**

6. Wählen Sie eine der folgenden Optionen aus und klicken Sie auf **Weiter**.

Ich verwende das Modul „Datenintegrität“ nicht	Wählen Sie diese Option aus, wenn die Daten aus dem zentralen Speicher nicht digital signiert und gesichert eingetragen werden müssen.
Ich verwende das Modul „Datenintegrität“	Wählen Sie diese Option aus, wenn die Daten aus dem zentralen Speicher digital signiert und gesichert eingetragen werden, und wenn dieses Dienstmodul zur Installation ausgewählt wird. • Geben Sie den Namen des Computers ein, der das Modul **Datenintegrität** hostet. • Wählen Sie einen Port für den Dienst aus. Die Standardportnummer ist 443. Weitere Informationen finden Sie unter „Portnummer für den Password Manager-Dienst“ auf Seite 112

Hinweis: Wenn Sie das Modul **Datenintegrität** zu einem späteren Zeitpunkt installieren oder die Konsole und die Agentsoftware installiert haben, müssen Sie die vorhandenen Daten im zentralen Speicher mit dem Datensignierungstool CtxSignData.exe digital signieren. (Dieses Tool steht nach der Installation des Moduls **Datenintegrität** zur Verfügung.)

Umgekehrt müssen Sie die Signierung der Daten im zentralen Speicher aufheben, wenn Sie das Modul **Datenintegrität** deinstallieren. Weitere Informationen zur Signatur von Daten finden Sie unter „Aktivieren und Deaktivieren des Datenintegritätsdienstes in der Password Manager Agent-Software“ im *Citrix Password Manager-Administratorhandbuch*.

Auf der angezeigten Seite **Domänen konfigurieren** wird eine Liste der Domänen angezeigt, die den Password Manager-Dienst unterstützen können.

7. Führen Sie die folgenden Schritte auf der Seite **Domänen konfigurieren** aus:

   A. Aktivieren Sie das Optionsfeld neben jeder Domäne, für die Sie die Dienstunterstützung aktivieren möchten.

   B. Wählen Sie eine Domäne oder mehrere aus und klicken Sie auf **Eigenschaften**, um das Dialogfeld **Konfiguration bearbeiten** zu öffnen.

   C. Wenn Sie einen zentralen Speicher unter Active Directory erstellt haben, klicken Sie auf **Active Directory** und wählen Sie den richtigen Domänencontroller aus der Liste aus.

   D. Klicken Sie auf **Datenproxykonto** und geben Sie den Benutzernamen, das Kennwort und die Domäne des Datenproxykontos ein, das für die Kommunikation mit dem zentralen Speicher verwendet wird.

   E. Wenn Sie das Self-Service-Modul installiert haben, klicken Sie auf **Self-Service-Konto** und geben Sie die Anmeldeinformationen für diese Funktion ein. Weitere Informationen finden Sie unter „Self-Service-Anforderungen“ auf Seite 85.

   F. Klicken Sie auf **OK**, um das Dialogfeld **Konfiguration bearbeiten** zu schließen.

   G. Klicken Sie auf **Weiter**.

Auf der Seite **Einstellungen bestätigen** werden die Eigenschaften für die Konfiguration des Dienstmoduls angezeigt. Klicken Sie auf **Zurück**, um Informationen zu ändern oder zu korrigieren.

8. Klicken Sie auf **Fertig stellen**, um die Dienstkonfigurationsinformationen zu senden. Klicken Sie erneut auf **Fertig stellen**, um das Dialogfeld **Einstellungen anwenden** zu schließen.

Portnummer für den Password Manager-Dienst

Die Standardportnummer für den Password Manager-Dienst ist 443. Wenn Sie den Password Manager-Dienst wie unter „So konfigurieren Sie die Password Manager-Dienste“ auf Seite 108 beschrieben konfigurieren, können Sie auch jeden anderen verfügbaren Port auf dem Dienstserver verwenden, wenn Port 443 bereits belegt ist.

Password Manager greift mit dieser Portnummer auf jedes installierte Dienstmodul zu.

- Wenn Sie später Dienstmodule installieren, müssen Sie die Portnummer verwenden, die bei der Erstinstallation des Dienstes festgelegt wurde.
- Der Dienst kann nicht an mehreren Ports ausgeführt werden. Wenn Sie den falschen Port angeben, kann dies später zu Fehlermeldungen vom Typ „Fehler bei der Kommunikation bzw. beim Herstellen einer Verbindung zum Password Manager-Dienst“ führen.
- Die Angabe der richtigen Dienstportnummer ist auch wichtig, wenn Sie das Signaturtool für die Datenintegrität an der Befehlszeile verwenden.

Installieren und Konfigurieren der Password Manager Console

Sie können die Konsole auf jedem Computer in der Umgebung installieren. Um Password Manager in einer Umgebung mit mehreren Domänen und mehreren zentralen Speichern zu verwenden, können Sie die Konsole auf einem beliebigen Computer in der Domäne installieren.

Installieren Sie das Anwendungsdefinitionstool auf jedem Computer in der Umgebung, wenn Sie Anwendungsdefinitionen im Standalone-Modus ohne vorherige Installation der Konsole erstellen möchten.

Bei den folgenden Schritten wird davon ausgegangen, dass die Password Manager-CD in den Computer eingelegt ist, der als Host für den zentralen Speicher dient, und dass der Autorun-Bildschirm angezeigt wird.

So installieren Sie die Password Manager Console

1. Klicken Sie auf **Schritt 3: Administrative Komponenten installieren**.
2. Klicken Sie auf **Schritt 3: Password Manager Console installieren**.
3. Klicken Sie auf **Weiter**, stimmen Sie der Lizenzvereinbarung zu und klicken Sie erneut auf **Weiter**.

   Das Dialogfeld **Installationstyp** wird angezeigt.

4. Wählen Sie die zu installierenden Komponenten aus und klicken Sie auf **Weiter**.

Konsole	Aktivieren Sie diese Option, um die Konsole zu installieren. Diese wird benötigt, um Richtlinien, Anwendungsdefinitionen, Benutzerkonfigurationen usw. zu erstellen und zu verwalten.
Anwendungs-definitionstool	Aktivieren Sie diese Option, um das Tool zu installieren, mit dem Sie Anwendungsdefinitionen erstellen können, ohne die Konsole starten oder verwenden zu müssen. Auf Computern, auf denen die Konsole nicht installiert ist bzw. nicht installiert werden kann, können Sie dieses Tool im Standalone-Modus verwenden.
Lizenzserver-Administration	Aktivieren Sie diese Option, um diese Komponente zur Unterstützung der Lizenzverwaltung auf der Konsole zu installieren. Mit dieser Option können Sie eine Verknüpfung zum Lizenzserver erstellen.
Access Management Console - Diagnostic Facility	Aktivieren Sie diese Option, um den Citrix Support bei der Behebung von Problemen mit der Konsole zu unterstützen.

5. Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**, wenn die Installation abgeschlossen ist.

Sie können nun die Konsole konfigurieren.

So konfigurieren Sie die Password Manager Console

Hinweis: Beim ersten Aufrufen der Konsole nach der Installation wird die Discovery durchgeführt und Sie können die Einstellungen der Konsole konfigurieren. Im Anschluss an diesen ersten Schritt können Sie jederzeit eine Discovery durchführen und die Konfigurationseinstellungen ändern, indem Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console** und anschließend im Bereich **Häufige Tasks** auf **Discovery konfigurieren und durchführen** klicken.

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.

   Das Dialogfeld **Discovery konfigurieren und durchführen** wird angezeigt.

2. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Produkte und Komponenten auswählen** wird angezeigt.

3. Klicken Sie auf **Citrix Ressourcen**, wählen Sie **Konfigurationstools** und **Password Manager** aus und klicken Sie auf **Weiter**.

4. Wählen Sie den zuvor erstellten zentralen Speicher aus und klicken Sie auf **Weiter**.

   Hinweis: Wenn Sie eine NTFS-Netzwerkfreigabe oder einen freigegebenen Novell Ordner als zentralen Speicher verwenden, geben Sie den UNC-Pfad zur Freigabe ein.

5. Führen Sie folgende Schritte auf der Seite **Datenintegrität konfigurieren** aus:

   - Wenn Sie das Modul **Datenintegrität** installiert und während der Dienstkonfiguration aktiviert haben, aktivieren Sie das Kontrollkästchen, geben Sie den Servernamen und die Portnummer in die Textfelder ein und klicken Sie auf **Weiter**.
   - Wenn Sie das Modul **Datenintegrität** installiert haben, aber nicht aktivieren möchten, klicken Sie auf **Weiter**, ohne das Kontrollkästchen zu aktivieren. Stellen Sie sicher, dass die Funktion zuerst im Assistenten für die Dienstkonfiguration auf dem Dienstcomputer deaktiviert wurde. Weitere Informationen finden Sie unter „So konfigurieren Sie die Password Manager-Dienste“ auf Seite 108.

   Das Dialogfeld **Discoveryvorschau** mit einer Zusammenfassung der Konfiguration angezeigt.

6. Klicken Sie auf **Weiter**, um mit der Discovery zu beginnen.
7. Wenn die Discovery erfolgreich abgeschlossen wurde, klicken Sie auf **Fertig stellen**.

Die Konsole ist nun einsatzbereit. Sie können nun mit der Konsole die Password Manager-Umgebung einrichten und die Agentsoftware an Benutzer verteilen.

Installieren und Konfigurieren von Password Manager Agent

Hinweis: Zu Testzwecken können Sie auch die Konsole und den Agent auf demselben Computer installieren, um sicherzustellen, dass Änderungen an der Konsole vom Agent übernommen werden. **(Dies gilt nicht für Computer, die unter Windows Vista ausgeführt werden)**

Wichtig: Sie müssen Benutzerkonfigurationen erstellen, bevor Sie die Agentsoftware auf Benutzerdesktops installieren. Wenn Sie die Agentsoftware installieren, ohne die Aufgaben unter „Erste Schritte“ auf Seite 21 auszuführen, wird Benutzern beim Start der Agentsoftware unter Umständen eine Fehlermeldung angezeigt.

Berücksichtigen Sie außerdem, dass die Agentsoftware, die auf 64-Bit-Computern ausgeführt wird, keine Verbindung zu zentralen Speichern in freigegebenen Novell Ordnern herstellen kann.

Password Manager Agent wird auf Clientgeräten ausgeführt, z. B. Desktopcomputer, Laptops, Handheldcomputer und andere Geräte. In diesem Fall stellt die Agentsoftware die Anmeldeinformationen sowie den Zugriff auf die lokal auf dem Clientgerät ausgeführten Anwendungen bereit.

Sie können die Agentsoftware auch auf einem Computer installieren, auf dem Citrix Presentation Server ausgeführt wird. In diesem Fall stellt die Agentsoftware die Anmeldeinformationen sowie den Zugriff auf die veröffentlichten Anwendungen bereit.

Benutzer können auch dann über die Agentsoftware auf lokale Anwendungen zugreifen, wenn sie nicht mit einem Netzwerk verbunden sind. Ihre Anmeldeinformationen werden dann synchronisiert, wenn sie erneut eine Verbindung mit dem Unternehmensnetzwerk herstellen.

Wenn Sie die Agentsoftware mit der Autorun-Option auf der Password Manager-CD installieren, wird von der Installationssoftware überprüft, welches Betriebssystem vorliegt (32 Bit oder 64 Bit, Windows Vista oder ein anderes unterstütztes Windows-Betiebssystem) und anschließend die entsprechende Agentsoftware installiert.

In diesem Abschnitt werden die folgenden Themen behandelt:

- „Installationsszenarios“ auf Seite 119
- „Überlegungen“ auf Seite 120
- „Erhalten der GINA-Kette bei der Agentinstallation“ auf Seite 128
- „So installieren Sie Password Manager Agent auf einem lokalen Client“ auf Seite 121
- „So erstellen Sie ein Image der Agentsoftware für die Netzwerkinstallation“ auf Seite 123
- „Installation von Password Manager Agent ohne Benutzereingriffe“ auf Seite 126

Installationsszenarios

In der folgenden Tabelle sind einige Umgebungen und Schemata für die Installation aufgeführt:

Presentation Server und Access Gateway	Presentation Server und Access Gateway bieten Anwendungen, auf die Benutzer über ihre Webbrowser zugreifen. Installieren Sie die Password Manager Agent-Software auf jedem Server, auf dem Presentation Server ausgeführt wird.
Gemischte Umgebungen	Benutzer greifen auf veröffentlichte und lokale Anwendungen zu. Installieren Sie die Password Manager Agent-Software auf jedem Server mit Presentation Server und auf jedem Desktop. Sie können die Agentsoftware auch mit Installation Manager für Presentation Server installieren.
Lokale Installation	Benutzer greifen auf Anwendungen zu, die auf lokalen Geräten installiert sind. Installieren Sie die Password Manager Agent-Software auf einem lokalen Clientgerät. Weitere Informationen finden Sie unter „So installieren Sie Password Manager Agent auf einem lokalen Client“ auf Seite 121.
Softwareimage für die Netzwerkinstallation	Erstellen Sie ein Installationsimage und stellen Sie es im Netzwerk zur Verfügung. Weitere Informationen finden Sie unter „So erstellen Sie ein Image der Agentsoftware für die Netzwerkinstallation“ auf Seite 123.
Agentinstallation ohne Benutzereingriffe	Verwenden Sie die Windows Installer-Optionen zur Agentinstallation. Weitere Informationen finden Sie unter „Installation von Password Manager Agent ohne Benutzereingriffe“ auf Seite 126.

Auf Clientgeräten zeigt das Symbol der Agentsoftware im Infobereich an, wie die Software bereitgestellt wird:

- Die Agentsoftware, die auf einem Clientgerät installiert ist, zeigt als Symbol im Infobereich einen Schlüssel auf blauem Hintergrund an.
- Die Agentsoftware, die auf einem Server mit Presentation Server veröffentlicht ist, zeigt als Symbol im Infobereich einen Schlüssel und Server auf blauem Hintergrund an.

Überlegungen

- Wenn Sie mehrere Citrix Produkte neu installieren, die auch Password Manager umfasst, installieren Sie Password Manager Agent zum Schluss.
- Wenn Sie den Speicherort des Lizenzservers oder andere lizenzierungsrelevante Parameter konfigurieren oder ändern, werden diese Änderungen nicht auf Instanzen der Agentsoftware angewendet, die in der Umgebung verwendet werden. Sie müssen die Agentsoftware beenden und neu starten, um die Änderungen zu übernehmen.
- Wenn Sie im Rahmen der Agentinstallation Hotdesktop in der Umgebung einsetzen möchten, lesen Sie die Informationen unter „Benutzererfahrung bei Hotdesktop“ auf Seite 52.
- **Dies gilt nicht für Computer, die unter Windows Vista ausgeführt werden:**Nach der Installation der Agentsoftware müssen Sie das Gerät neu starten, damit die GINA-DLL installiert werden kann. Weitere Informationen zu GINA finden Sie unter „Erhalten der GINA-Kette bei der Agentinstallation“ auf Seite 128.

  Die Agentsoftware kann erst nach dem Neustart der Arbeitsstation ausgeführt werden. Wenn Sie die Arbeitsstation nicht sofort neu starten möchten, können Sie den Neustart auch unterdrücken. Verwenden Sie den optionalen Parameter `/norestart` mit dem Befehl `msiexec` des Microsoft Installer-Pakets, um den Neustart zu unterdrücken. Verwenden Sie folgenden Befehl, um das Installer-Paket mit der Funktion zum Unterdrücken auszuführen:

  msiexec /norestart /i *Pfad zur MSI-Datei einschließlich Dateinamen*

  Um eine vollständige Liste der Windows Installer-Optionen anzuzeigen, öffnen Sie auf einer Arbeitsstation mit installiertem Windows Installer eine Eingabeaufforderung und geben Sie Folgendes ein:

  msiexec /?

So installieren Sie Password Manager Agent auf einem lokalen Client

Hinweis: Wenn Sie im Rahmen der Agentinstallation Hotdesktop in der Umgebung einsetzen möchten, lesen Sie die Informationen unter „Benutzererfahrung bei Hotdesktop“ auf Seite 52.

Bei den folgenden Schritten wird davon ausgegangen, dass die Password Manager-CD in den Computer eingelegt ist, auf dem die Agentsoftware installiert wird, und dass das Autorun-Dialogfeld angezeigt wird.

1. Klicken Sie auf **Schritt 4: Password Manager Agent-Software installieren.**
2. Klicken Sie auf **Password Manager Agent installieren**.

   Der **Installationsassistent von Password Manager Agent** wird angezeigt.
3. Klicken Sie auf **Weiter**, stimmen Sie der Lizenzvereinbarung zu und klicken Sie erneut auf **Weiter**.

   Das Dialogfeld **Funktionsauswahl** wird angezeigt.
4. Wählen Sie die optionalen Komponenten aus, die installiert werden, und klicken Sie auf **Weiter**.

   - Datenintegrität (wenn Sie diesen Dienst installiert haben)
   - Self-Service (wenn Sie diesen Dienst installiert haben)
   - Hotdesktop (für diese Option muss ein Konto zur Verwendung als Hotdesktop-Konto vorhanden sein)

     Hinweis: Hotdesktop wird nicht unter Windows Vista, allen Plattformen mit ausgeführten Terminaldiensten, allen Serverbetriebssystemen oder einem 64-Bit-Betriebssystem unterstützt
   - Java-Unterstützung (zur Installation der Password Manager-Unterstützung für die Java Runtime Environment (JRE), die bereits auf dem Client installiert ist)

   Das Dialogfeld **Zentralen Speicher konfigurieren** wird angezeigt.

5. Geben Sie auf der Seite **Zentralen Speicher konfigurieren** Folgendes an:

   A. Wählen Sie den Typ des zentralen Speichers.

   B. Geben Sie bei Auswahl von **NTFS-Netzwerkfreigabe** oder **Freigegebener Novell Ordner** den Speicherort des zentralen Speichers ein.

   C. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Serveradresse angeben** wird angezeigt.

6. Geben Sie die Adresse und die Portnummer des Hostcomputers für den Dienst ein und klicken Sie auf **Weiter**.

   Geben Sie im Textfeld für die Adresse den vollqualifizierten Domänennamen des Dienstcomputers ein. Die Standardportnummer ist 443. Weitere Informationen finden Sie unter „Portnummer für den Password Manager-Dienst“ auf Seite 112.

   Wenn Sie Hotdesktop ausgewählt haben, wird das Dialogfeld **Hotdesktop-Konto konfigurieren** angezeigt.

   Hinweis: Wenn Sie Hotdesktop verwenden, dürfen weder Remotedesktop noch die Terminaldienste ausgeführt werden. Während der Hotdesktop-Installation setzt das Installationsprogramm den Wert des Registrierungsschlüssels AllowMultipleSessions auf 0 zurück.

   ---

7. Geben Sie die Anmeldeinformationen des Benutzers für das Hotdesktop-Konto ein und klicken Sie auf **Weiter**.

   Geben Sie den Namen der Domäne an, zu der die Arbeitsstation gehört. Verwenden Sie dabei den NetBIOS-Namen der Domäne und nicht den vollqualifizierten Domänennamen.

8. Klicken Sie auf **Installieren**.

9. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.

10. Führen Sie einen der folgenden Schritte aus:

    - Wenn Sie ein unterstütztes Betriebssystem außer Windows Vista verwenden, klicken Sie auf **Ja**, um das Clientgerät neu zu starten. Sie müssen das Clientgerät neu starten. Weitere Informationen finden Sie unter „Überlegungen“ auf Seite 120 und „Erhalten der GINA-Kette bei der Agentinstallation“ auf Seite 128.
    - Unter Windows Vista müssen Sie sich vom Windows Vista-Konto ab- und dann erneut anmelden. Ein Neustart des Clientgeräts ist nicht erforderlich.

So erstellen Sie ein Image der Agentsoftware für die Netzwerkinstallation

---

Wichtig: Wenn Sie ein Image von einem 32-Bit-Computer erstellen, kann dieses nur auf 32-Bit-Computern installiert werden. Wenn Sie ein Image von einem 64-Bit-Computer erstellen, kann dieses nur auf 64-Bit-Computern installiert werden.

Sie können mit einem Dienstprogramm auf der Produkt-CD ein Image der Agentsoftware auf einer Netzwerkfreigabe installieren. Mit diesem Dienstprogramm wird ein Installationsimage von Password Manager Agent erstellt, das die benutzerdefinierten Parameter enthält. Bei den folgenden Schritten wird davon ausgegangen, dass die Password Manager-CD in den Computer eingelegt ist, auf dem die Agentsoftware installiert wird, und dass das Autorun-Dialogfeld angezeigt wird.

Hinweis: Wenn Sie im Rahmen der Agentinstallation Hotdesktop in der Umgebung einsetzen möchten, lesen Sie die Informationen unter „Benutzererfahrung bei Hotdesktop“ auf Seite 52.

---

1. Klicken Sie auf **Schritt 4: Password Manager Agent-Software installieren.**
2. Klicken Sie auf **Password Manager Agent-Installationsimage erstellen**.

   Der **Installationsassistent von Password Manager Agent** wird angezeigt.
3. Klicken Sie auf **Weiter**.
4. Geben Sie im Dialogfeld **Administratives Installationspaket erstellen** den Speicherort auf der Netzwerkfreigabe für das Installationspaket ein und klicken Sie auf **Weiter**.

5. Wählen Sie die optionalen Komponenten aus, die installiert werden, und klicken Sie auf **Weiter**.

   - Datenintegrität (wenn Sie diesen Dienst installiert haben)
   - Self-Service (wenn Sie diesen Dienst installiert haben)
   - Hotdesktop (für diese Option muss ein Konto zur Verwendung als Hotdesktop-Konto vorhanden sein)

   Hinweis: Hotdesktop wird nicht unter Windows Vista, allen Plattformen mit ausgeführten Terminaldiensten, allen Serverbetriebssystemen oder einem 64-Bit-Betriebssystem unterstützt

   - Java-Unterstützung (zur Installation der Password Manager-Unterstützung für die Java Runtime Environment (JRE), die bereits auf dem Client installiert ist)

   Das Dialogfeld **Zentralen Speicher konfigurieren** wird angezeigt.

6. Geben Sie auf der Seite **Zentralen Speicher konfigurieren** Folgendes an:

   A. Wählen Sie den Typ des zentralen Speichers.

   B. Geben Sie bei Auswahl von **NTFS-Netzwerkfreigabe** oder **Freigegebener Novell Ordner** den Speicherort des zentralen Speichers ein.

   C. Klicken Sie auf **Weiter**.

   Die Seite **Citrix Password Manager-Dienstkonfiguration** wird angezeigt.

7. Geben Sie die Adresse und die Portnummer des Hostcomputers für den Dienst ein und klicken Sie auf **Weiter**.

   Geben Sie im Textfeld für die Adresse den vollqualifizierten Domänennamen des Dienstcomputers ein. Die Standardportnummer ist 443. Weitere Informationen finden Sie unter „Portnummer für den Password Manager-Dienst“ auf Seite 112.

Wenn Sie Hotdesktop ausgewählt haben, wird das Dialogfeld **Hotdesktop-Konto konfigurieren** angezeigt.

Hinweis: Wenn Sie Hotdesktop verwenden, dürfen weder Remotedesktop noch die Terminaldienste ausgeführt werden. Während der Hotdesktop-Installation setzt das Installationsprogramm den Wert des Registrierungsschlüssels AllowMultipleSessions auf 0 zurück.

---

8. Geben Sie die Anmeldeinformationen des Benutzers für das Hotdesktop-Konto ein und klicken Sie auf **Weiter**. Geben Sie den Namen der Domäne an, zu der die Arbeitsstation gehört. Verwenden Sie dabei den NetBIOS-Namen der Domäne und nicht den vollqualifizierten Domänennamen.
9. Klicken Sie im Dialogfeld **Fertig mit Überprüfen der Administratorinstallation** auf **Weiter**.
10. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.

Die Datei Setup.msi und unterstützende Dateien sind nun im angegebenen Verzeichnis auf der Netzwerkfreigabe gespeichert.

Wichtig: Bevor Sie Password Manager Agent auf einem Computer unter Windows Vista von einer Befehlszeile aus installieren, müssen Sie zuerst die aktualisierten C-Laufzeitbibliotheken von der Produkt-CD installieren. Die Installation schlägt ohne die aktualisierten C-Laufzeitbibliotheken fehl. Weitere Informationen finden Sie unter „Installation von Password Manager Agent ohne Benutzereingriffe“ auf Seite 126.

Installation von Password Manager Agent ohne Benutzereingriffe

Mit der Windows Installer-Option /quiet können Sie Password Manager Agent ohne Benutzereingriffe an der Befehlszeile installieren.

So installieren Sie Password Manager Agent ohne Benutzereingriff von der Befehlszeile aus

Wichtig: Bevor Sie Password Manager Agent auf einem Computer unter Windows Vista von einer Befehlszeile aus installieren, müssen Sie zuerst die aktualisierten C-Laufzeitbibliotheken von der Produkt-CD installieren. Die Installation schlägt ohne die aktualisierten C-Laufzeitbibliotheken fehl.

1. Nur Computer mit Windows Vista: Führen Sie folgende Schritte aus:
   - 32-Bit-Computer: Führen Sie Agent\Vcredist_x86.exe von der Produkt-CD aus.
   - 64-Bit-Computer: Führen Sie Agent\Vcredist_x86.exe und Agent\X64\vcredist_x64.exe von der Produkt-CD aus.
2. Gehen Sie an der Befehlszeile auf die Netzwerkfreigabe, auf der das Password Manager-Image (Setup.msi) gespeichert ist.
3. Geben Sie **setup.msi /quiet** ein.

Andere Befehlszeilenparameter stehen zur Verfügung. Um eine vollständige Liste der Windows Installer-Optionen anzuzeigen, öffnen Sie auf einer Arbeitsstation mit installiertem Windows Installer eine Eingabeaufforderung und geben Sie Folgendes ein:

msiexec /?

In der folgenden Tabelle sind die Password Manager-spezifischen Optionen aufgeführt, die bei der Installation von Password Manager an der Befehlszeile verwendet werden. Für jede Option ist ein Gleichheitszeichen (=) zum Festlegen der Werte erforderlich (Beispiel: SSPR_SELECT=1 aktiviert die Self-Service-Funktionen).

Option	**Beschreibung:**
SYNCPOINTTYPE	Gibt den Typ des zentralen Speichers an. Geben Sie `FileSyncPath` an, um eine NTFS-Netzwerkfreigabe als zentralen Speicher zu verwenden. Geben Sie `ADSyncPath` an, um einen zentralen Speicher unter Active Directory zu verwenden. Geben Sie `NovellSyncPath` an, um einen freigegebenen Novell Ordner als zentralen Speicher zu verwenden.
SYNCPOINTLOC	Gibt den UNC-Pfad für die NTFS-Netzwerkfreigabe an, die als zentraler Speicher verwendet wird. Geben Sie *Servername**Ordnername*$ an, wobei *Servername* der Name des Hostcomputers für den zentralen Speicher und *Ordnername* der Name des freigegebenen Ordners ist. Für zentrale Speicher unter Active Directory ist diese Option nicht erforderlich.
DI_SELECT	Geben Sie 1 an, um die Datenintegritätsfunktion zu aktivieren.
SSPR_SELECT	Geben Sie 1 an, um die Self-Service-Funktion zu aktivieren.
SERVICEURL	Gibt die URL des Dienstservers an. Geben Sie *FQDN*\MPMService an, wobei *FQDN* der vollqualifizierte Domänenname für den Dienstserver ist. Diese Option wird benötigt, wenn Sie DI_SELECT und/oder SSPR_SELECT angegeben haben.
SERVICEURLPORT	Gibt den Port des Dienstservers an. Der Standardport ist 443. Weitere Informationen finden Sie unter „Portnummer für den Password Manager-Dienst“ auf Seite 112. Diese Option wird benötigt, wenn Sie DI_SELECT und/oder SSPR_SELECT angegeben haben.

/forcerestart	Geben Sie /forcerestart an, um die Arbeitsstation nach der Installation zu beenden und neu zu starten. Für die Installation der Agentsoftware ist ein Neustart erforderlich. Geben Sie **msiexec /?** ein, um weitere Optionen anzuzeigen. Sie können auch REBOOT="" verwenden.
Hotdesktop-spezifische Optionen	Sie auch „Hotdesktop: Desktopfreigabeumgebung für Benutzer" im *Citrix Password Manager-Administratorhandbuch*.
HD_SELECT	Geben Sie 1 an, um Hotdesktop zu installieren.
HD_USERNAME	Gibt den Benutzernamen für das Hotdesktop-Konto an.
HD_PASSWORD	Gibt das Kennwort für das Hotdesktop-Konto an.
HD_DOMAIN	Gibt die Domäne für das Hotdesktop-Konto an.
DISABLE_TERMINAL_SERVICE	Geben Sie 1 an, um die Terminaldienste zu deaktivieren. Dies ist für die Verwendung von Hotdesktop erforderlich.

Erhalten der GINA-Kette bei der Agentinstallation

Wichtig: Wenn Sie ein Password Manager-Image von einem 32-Bit-Computer erstellen, kann dieses nur auf 32-Bit-Computern installiert werden. Wenn Sie ein Image von einem 64-Bit-Computer erstellen, kann dieses nur auf 64-Bit-Computern installiert werden.

Hinweis: Windows Vista verwendet die GINA-Funktionalität nicht. Dieser Abschnitt gilt nicht für Computer, die unter Windows Vista ausgeführt werden.

Graphical Identification and Authentication (GINA) ist die Windows-Komponente, die das Dialogfeld steuert, das Benutzern angezeigt wird, wenn sie die Tastenkombination STRG+ALT+ENTF drücken. Das Dialogfeld sammelt alle für die Authentifizierung erforderlichen Daten. Presentation Server, Password Manager und der Novell NetWare-Client interagieren alle mit der Microsoft GINA-DLL (Dynamic Link Library) bzw. machen eine Ersetzung erforderlich.

Wenn Sie eine andere Software installieren, die eine benutzerdefinierte GINA-DLL verwendet, stellen Sie unbedingt sicher, dass die GINA-Kette nicht unterbrochen wird. Unter Umständen müssen Sie Software in einer bestimmten Reihenfolge installieren oder deinstallieren, damit die richtige GINA-Kette erhalten bleibt. Wenn Sie Password Manager Agent zuletzt installieren, gewährleisten Sie, dass die Password Manager-GINA zu Beginn des Winlogon-Prozesses aufgerufen wird.

Konfigurieren und Verwenden der Mehrdomänendienstfunktion

Mit Citrix Password Manager 4.6 können Sie den Password Manager-Dienst für Benutzer in verschiedenen, jedoch vertrauenswürdigen Domänen gemeinsam verwenden. Ein Administrator kann die Password Manager Console auf Computern in verschiedenen Domänen installieren und Benutzerkonfigurationen in jeder Domäne erstellen.

Beispiel: Der Computer mit dem Password Manager-Dienst befindet sich in DomäneA. Benutzer, die einer Benutzerkonfiguration in DomäneA zugeordnet sind, können mit dem Konto-Self-Service die Sperrung der Konten aufheben. Benutzer, die einer Benutzerkonfiguration in DomäneB zugeordnet sind, können diese vom Dienstcomputer der DomäneA bereitgestellte Funktion auch verwenden. In dieser Situation bestehen mehrere Benutzerkonfigurationen in mehreren Domänen, die einen Computer mit dem Password Manager-Dienst für diese Funktion verwenden.

Anforderungen

Vor der Implementierung der Mehrdomänendienstfunktion müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind:

Komponente	Anforderung
Domänen	Jede Domäne, die den Dienst gemeinsam verwendet, muss zu derselben Domänenstruktur gehören. Die Domänen in der Struktur müssen eine gegenseitige Vertrauensbeziehung haben.

Komponente	Anforderung
Zentraler Speicher	Diese Funktion kann implementiert werden, wenn als zentraler Speicher Active Directory oder eine NTFS-Netzwerkfreigabe verwendet wird. Die Funktion steht nicht zur Verfügung, wenn Sie als zentralen Speicher einen freigegebenen Novell Ordner verwenden. Alle Benutzer, die denselben Dienstcomputer gemeinsam verwenden, müssen denselben Typ des zentralen Speichers verwenden: Active Directory oder freigegebener NTFS-Ordner. Mehrere Typen des zentralen Speichers werden nicht unterstützt. In dieser Situation kann als zentraler Speicher kein freigegebener NTFS-Ordner pro Domäne verwendet werden. Sie können jedoch als zentralen Speicher einen freigegebenen NTFS-Ordner pro Struktur verwenden.
Datenintegrität	Die Datenintegrität muss konsistent domänenübergreifend verwendet werden. Das heißt, die Funktion ist entweder in der Konfiguration der Dienst- und Agentsoftware für alle Domänen aktiviert oder deaktiviert. Beispiel: Sie können diese Funktion nicht in der Dienstkonfiguration aktivieren und bei der Installation der Agentsoftware deaktivieren.
Password Manager Console	Jede Konsole kann nur einen zentralen Speicher und nicht mehrere zentrale Speicher anzeigen. Der Password Manager Administrator sollte eine Konsole in jeder Domäne mit einem Benutzerkonto installieren, das administrative Rechte in der Domäne hat. Der Administrator kann auch eine Konsole installieren, die auf andere Domänen zugreifen kann. Er kann dann ggf. zu einer dieser Domänen wechseln, wenn er sich mit den Anmeldeinformationen für diese Domäne anmeldet.
Datenproxy und Self-Service-Konten	Sie können einen Datenproxy und ein Self-Service-Konto konfigurieren, das Lese- und Schreibrechte für den zentralen Speicher und ausreichende Privilegien für das Zurücksetzen der Benutzerkennwörter und das Aufheben der Kontosperrung hat. Sie können diese Konten auch für jede Domäne im Dienstkonfigurationstool angeben.

Taskübersicht

Führen Sie die folgenden Tasks für die Implementierung der Mehrdomänendienstfunktion aus.

Aufgabe	Beschreibung/Siehe Abschnitt
Installieren Sie eine Instanz der Konsole in jeder Domäne, in der diese Funktion verwendet wird, und erstellen Sie Benutzer-konfigurationen.	„Installieren und Verwenden der Password Manager Console und des Anwendungsdefinitionstools“ auf Seite 86
Konfigurieren Sie den Dienst.	„So konfigurieren Sie den Dienst für mehrere Domänen“ auf Seite 131

So konfigurieren Sie den Dienst für mehrere Domänen

1. Melden Sie sich als Administrator am Computer an, auf dem der Dienst installiert ist.
2. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Password Manager** > **Dienstkonfiguration**, um das Dienstkonfigurationstool zu starten.
3. Wenn das Dienstkonfigurationstool angezeigt wird, klicken Sie im linken Bereich auf **Domänenkonfigurationen**.

   Eine Liste der Domänen wird angezeigt.
4. Markieren Sie das Optionsfeld neben jeder Domäne, um die Dienstunterstützung für diese Domäne zu aktivieren.
5. Wählen Sie eine Domäne oder mehrere aus und klicken Sie auf **Eigenschaften**, um das Dialogfeld **Konfiguration bearbeiten** zu öffnen.
6. Klicken Sie auf **Datenproxykonto** und geben Sie den Benutzernamen, das Kennwort und die Domäne des Datenproxykontos ein, das für die Kommunikation mit dem zentralen Speicher verwendet wird.
7. Wenn Sie das Self-Service-Modul installiert haben, klicken Sie auf **Self-Service-Konto** und geben Sie die Anmeldeinformationen für diese Funktion ein. Weitere Informationen finden Sie unter „Self-Service-Anforderungen“ auf Seite 85.
8. Klicken Sie auf **OK**, um das Dialogfeld **Konfiguration bearbeiten** zu schließen.
9. Klicken Sie auf **OK**, um die Konfiguration zu speichern.

Aktualisieren von Password Manager

Wichtig: Installieren Sie Password Manager nicht auf Domänencontrollern. Das Installieren einer Komponente von Password Manager (Agent, Dienst, Konsole oder zentraler Speicher) auf einem Domänencontroller wird nicht unterstützt.

In diesem Abschnitt werden die erforderlichen Schritte zum Aktualisieren von Citrix Password Manager von einer früheren Version auf die aktuelle Version 4.6 beschrieben:

- „Unterstützte Upgradepfade“ auf Seite 134
- „Zusammenfassung der Upgrade-Schritte“ auf Seite 134
- „Vor dem Upgrade von Password Manager“ auf Seite 135
- „Schritt 1: Aktualisieren des Password Manager-Dienstes“ auf Seite 141
- „Schritt 2: Aktualisieren der Password Manager Console“ auf Seite 143
- „Schritt 3: Aktualisieren von Password Manager Agent“ auf Seite 146

Unterstützte Upgradepfade

Die folgenden Versionen von Password Manager können auf Version 4.6 aktualisiert werden:

- Password Manager 4.1 (einschließlich aller Service Packs und Hotfixes)
- Password Manager 4.5 (einschließlich aller Hotfixe)

Wichtig: Nur die Versionen 4.1 und 4.5 können auf Password Manager 4.6 aktualisiert werden. Direkte Upgrades von Version 2.5 und 4.0 werden nicht unterstützt.

Zusammenfassung der Upgrade-Schritte

Aufgabe	Siehe Abschnitt oder Dokument
Vor dem Upgrade	
Bestimmen Sie, auf welchen Computern in der Umgebung die Software aktualisiert wird.	• „Planen der Password Manager-Umgebung“ auf Seite 19 • „Hardware- und Softwareanforderungen“ auf Seite 77
Bereiten Sie die Computer auf das Upgrade vor und exportieren Sie alle administrativen Daten.	• „Vor dem Upgrade von Password Manager“ auf Seite 135 • „Verschieben von Daten in einen anderen zentralen Speicher“ im *Citrix Password Manager-Administratorhandbuch* • „Sichern von Dateien des Password Manager-Dienstes“ im *Citrix Password Manager-Administratorhandbuch*
Erstellen Sie eine Sicherungskopie des zentralen Speichers. Erstellen Sie auf allen Hotdesktop-Arbeitsstationen eine Sicherungskopie der Datei process.xml.	„Vor dem Upgrade von Password Manager“ auf Seite 135
Installieren Sie den Lizenzserver und fügen Sie Lizenzen für Password Manager hinzu.	• „Lizenzierungsanforderungen“ auf Seite 92 • Handbuch *Schnelleinstieg für die Citrix Lizenzierung*, das auf der Citrix Website (http://www.citrix.com) verfügbar ist
Upgrade	
Prüfen Sie das Menü **Autorun**.	„Vor der Installation von Password Manager“ auf Seite 93
Aktualisieren Sie den Password Manager-Dienst.	„Schritt 1: Aktualisieren des Password Manager-Dienstes“ auf Seite 141

Aufgabe	Siehe Abschnitt oder Dokument
Aktualisieren Sie die Password Manager Console.	„Schritt 2: Aktualisieren der Password Manager Console“ auf Seite 143
Aktualisieren Sie den zentralen Speicher.	• „Auswählen des Typs des zentralen Speichers“ auf Seite 23 • „Schritt 2: Aktualisieren der Password Manager Console“ auf Seite 143
Aktualisieren Sie Password Manager Agent.	• „Schritt 3: Aktualisieren von Password Manager Agent“ auf Seite 146 • „Installieren und Konfigurieren von Password Manager Agent“ auf Seite 117

Vor dem Upgrade von Password Manager

Beachten Sie folgende Punkte, bevor Sie Password Manager aktualisieren:

- „Aktualisieren vorhandener Benutzerkonfigurationen“ im *Citrix Password Manager-Administratorhandbuch*
- „Sichern von wichtigen Dateien“ im *Citrix Password Manager-Administratorhandbuch*
- „Sichern von Dateien des Password Manager-Dienstes“ im *Citrix Password Manager-Administratorhandbuch*
- „Kontoanforderungen zum Installieren und Verwenden von Password Manager“ auf Seite 86
- „Verwenden von Autorun“ auf Seite 136
- „Upgradereihenfolge“ auf Seite 136
- „Verwenden des Tools CtxMoveKeyRecoveryData zum Sichern von Dienstdaten“ auf Seite 137
- „Sichern der Datei process.xml (nur in Hotdesktop-Umgebungen)“ auf Seite 138
- „Sichern des vorhandenen zentralen Speichers“ auf Seite 138
- „Aktualisierte Richtlinien, Anwendungsdefinitionen, Fragen/Fragenkataloge und Benutzerkonfigurationen“ auf Seite 139
- „Microsoft .NET Version 1.1 und 2.0“ auf Seite 140

Verwenden von Autorun

Mit Autorun können Sie verschiedene Password Manager-Aufgaben ausführen, zum Beispiel einen zentralen Speicher erstellen oder Komponenten von Password Manager aktualisieren. Wenn Sie die Produkt-CD in das CD-ROM-Laufwerk eingelegt haben, wird das Autorun-Dialogfeld angezeigt.

Wenn dieses Dialogfeld nicht automatisch angezeigt wird, gehen Sie wie folgt vor:

1. Öffnen Sie Windows Explorer und wählen Sie das CD-ROM-Laufwerk aus.
2. Klicken Sie auf Autorun.exe.

Upgradereihenfolge

Es wird empfohlen, Password Manager in der folgenden Reihenfolge zu aktualisieren:

- Installieren Sie die Lizenzen. (Weitere Informationen finden Sie unter „Lizenzierungsanforderungen“ auf Seite 92.)
- Aktualisieren Sie den Password Manager-Dienst, wenn Sie mindestens eines der folgenden Module verwenden:
    - Schlüsselverwaltung
    - Self-Service
    - Provisioning
    - Synchronisierung der Anmeldeinformationen
    - Datenintegrität

Hinweis: An dieser Stelle können Sie auch zusätzliche Module installieren. Lesen Sie vor der Installation die Informationen unter „Sicherheits- und Kontoanforderungen für den Password Manager-Dienst“ auf Seite 81.

Wenn Sie das Modul **Datenintegrität** zu einem späteren Zeitpunkt installieren möchten oder die Konsole und die Agentsoftware installiert haben, müssen Sie die vorhandenen Daten im zentralen Speicher mit dem Datensignierungstool CtxSignData.exe digital signieren. (Dieses Tool steht nach der Installation des Moduls **Datenintegrität** zur Verfügung.) Umgekehrt müssen Sie die Signierung der Daten im zentralen Speicher aufheben, wenn Sie das Modul **Datenintegrität** deinstallieren. Weitere Informationen zur Signatur von Daten finden Sie unter „Aktivieren und Deaktivieren des Datenintegritätsdienstes in der Password Manager Agent-Software“ im *Citrix Password Manager-Administratorhandbuch*.

- Aktualisieren Sie die Password Manager Console auf einem oder mehreren Computern in Ihrer Umgebung.
- Wenn Sie nur Anwendungsdefinitionen erstellen möchten, aktualisieren oder installieren Sie das Anwendungsdefinitionstool auf den Computern in der Umgebung.
- Wenn Sie die Password Manager-Funktionen in der Konsole konfiguriert haben, aktualisieren oder installieren Sie Password Manager Agent auf allen Benutzercomputern in der Umgebung.

Verwenden des Tools CtxMoveKeyRecoveryData zum Sichern von Dienstdaten

Wenn Sie die Dienstdaten mit dem Tool ctxmovekeyrecoverydata.exe gesichert haben, müssen Sie dieses Tool auch zum Wiederherstellen oder Importieren der Dienstdaten zum Dienstserver verwenden. Dieses Tool stand in Password Manager 4.1 zur Verfügung.

Wichtig: Das Tool CtxMoveServiceData.exe aus der Version 4.6 kann nicht zum Importieren von Dienstdaten verwendet werden, die mit dem Tool ctxmovekeyrecoverydata.exe exportiert (gesichert) wurden. Wenn dies versucht wird, werden die Dienstdaten beschädigt. Weitere Informationen finden Sie unter „Sichern von Dateien des Password Manager-Dienstes“ im *Citrix Password Manager-Administratorhandbuch*

Sichern der Datei process.xml (nur in Hotdesktop-Umgebungen)

Wenn Sie die Hotdesktop-Funktion schon einmal verwendet haben, müssen Sie eine Sicherungskopie der Datei process.xml erstellen. Diese befindet sich auf allen Hotdesktop-Arbeitsstationen im Ordner C:\Programme\Citrix\Metaframe Password Manager\HotDesktop.

Die vorhandene Datei process.xml file wird beim Upgrade gespeichert; Sie sollten diese Informationen jedoch unbedingt schützen.

Sichern des vorhandenen zentralen Speichers

Citrix empfiehlt, eine Sicherungskopie des vorhandenen zentralen Speichers zu erstellen. Ein zentraler Speicher der Version 4.1 oder 4.5 kann zwar nicht mit Password Manager 4.6 verwendet werden, dennoch sollten Sie den zentralen Speicher für den Fall sichern, dass die zuvor installierte Version von Passwort Manager wiederhergestellt werden muss. Umgekehrt ist es auch nicht möglich, einen zentralen Speicher der Version 4.6 mit der Password Manager-Version 4.1 oder 4.5 zu verwenden.

Hinweis: Password Manager Agent 4.1 und 4.5 kann mit einem zentralen Speicher von Password Manager 4.6 verwendet werden. Jedoch stehen die neuen Funktionen der Version 4.5 in diesen Versionen der Agentsoftware nicht zur Verfügung. Citrix empfiehlt, die Agentsoftware möglichst zu aktualisieren, damit sie mit den Versionen des Dienstes und der Konsole übereinstimmt. Durch Upgrades wird sichergestellt, dass den Benutzern immer die jeweils aktuellen Funktionen und Sicherheitsverbesserungen zur Verfügung stehen.

Aktualisierte Richtlinien, Anwendungsdefinitionen, Fragen/Fragenkataloge und Benutzerkonfigurationen

Hinweis: Weitere Informationen finden Sie unter „Aktualisieren vorhandener Benutzerkonfigurationen“ im *Citrix Password Manager-Administratorhandbuch*

Bei der ersten Durchführung und Konfiguration der Discovery in der aktualisierten Konsole für Password Manager 4.6 können Sie den zentralen Speicher (und die Daten im zentralen Speicher) aktualisieren. Die bestehenden Richtlinien, Fragen, Fragenkataloge, Anwendungsdefinitionen und Benutzerkonfigurationen bleiben erhalten.

Citrix empfiehlt, die Agentsoftware überall auf die jeweils aktuelle Version zu aktualisieren, um den Benutzern neue Funktionen und Sicherheitsverbesserungen zur Verfügung zu stellen. Aus dem gleichen Grund sollten Sie die Richtlinien, Anwendungsdefinitionen und Benutzerkonfigurationen ändern.

Microsoft .NET Version 1.1 und 2.0

Auf einer Arbeitsstation oder einem Server mit .NET 1.1 kann .NET 2.0 zusätzlich installiert werden. Dies wird als „Side-by-Side“-Installation des Framework bezeichnet. .NET 1.1 Framework muss auf keinem der Computer in Ihrer Umgebung deinstalliert werden. Weitere Informationen finden Sie unter „Installieren von Microsoft .NET 2.0 Framework“ auf Seite 88.

Wichtig: Bei früheren Versionen der Access Management Console musste Version 1.1 von Microsoft .NET Framework installiert werden. Für Computer, auf denen auch neuere Versionen von .NET Framework installiert waren, stellte Citrix die Datei mmc.exe.config zur Verfügung, mit der sichergestellt werden konnte, dass Version 1.1 ebenfalls geladen wird. Weitere Informationen finden Sie im entsprechenden Artikel in der Citrix Knowledge Base unter http://support.citrix.com/article/CTX108538.

Diese Datei wird nicht mehr benötigt und muss entfernt werden. Wenn Sie die Datei nicht entfernen, startet die Konsole nicht, und es wird eine Fehlermeldung wie z. B. „Fehler bei Initialisierung des Snap-Ins“ angezeigt. Löschen Sie die Datei \Windows\system32\mmc.exe.config (falls vorhanden), um dieses Problem zu umgehen.

Durch diese Maßnahme wird verhindert, dass frühere Versionen der Konsole aktiv sind (da diese nur mit Version 1.1 von .NET Framework funktionieren). Wenn Sie frühere Versionen verwenden und diese nicht aktualisieren möchten, wenden Sie sich an den technischen Support von Citrix. Dieser kann Ihnen eine alternative Problemlösung zur Verfügung stellen.

Schritt 1: Aktualisieren des Password Manager-Dienstes

Wenn Sie den Password Manager-Dienst verwenden, müssen Sie alle verwendeten Module des Dienstes gleichzeitig aktualisieren.

Beim Upgrade müssen Sie dienstspezifische Informationen angeben, z. B. Einstellungen, Benutzername und Kennwort für das Dienstkonto und den Speicherort des zentralen Speichers. Weitere Informationen finden Sie unter „So konfigurieren Sie die Password Manager-Dienste“ auf Seite 108.

Wichtig: In dieser Version von Password Manager können lokale Benutzerkonten nicht als Dienstkonto definiert werden. Weitere Informationen finden Sie unter „Anforderungen für Dienstkonten“ auf Seite 84.

Wenn der Dienst und die Konsole auf demselben Computer installiert sind, müssen beide aktualisiert werden.

Hinweis: Wenn Sie den Password Manager-Dienst nicht in der Password Manager 4.1- oder 4.5-Umgebung verwenden, müssen Sie nur die Konsole, den zentralen Speicher und die Agentsoftware aktualisieren.

Bei den folgenden Schritten wird davon ausgegangen, dass die Password Manager-CD in den Computer eingelegt ist, der als Host für den zentralen Speicher dient, und dass der Autorun-Bildschirm angezeigt wird.

So aktualisieren Sie den Password Manager-Dienst

1. Klicken Sie auf **Schritt 3: Administrative Komponenten installieren**.
2. Klicken Sie auf **Schritt 2: Password Manager-Dienst installieren (falls zutreffend)**.
3. **Nur für ein Upgrade von Version 4.1:** Klicken Sie im Bestätigungsdialogfeld auf **Ja**, um die vorherige Version des Dienstes zu entfernen und die Installation fortzusetzen.

   Nur für ein Upgrade von Version 4.1: Klicken Sie im Bestätigungsdialogfeld auf **Ja**, in dem Sie darauf hingewiesen werden, dass Sie nach dem Upgrade des Dienstes ein Upgrade der Password Manager Console durchführen müssen.
4. Klicken Sie auf **Weiter**, stimmen Sie der Lizenzvereinbarung zu und klicken Sie erneut auf **Weiter**.

5. Wählen Sie im Dialogfeld **Module auswählen** die Module aus, die Sie installieren möchten:
   - Schlüsselverwaltung
   - Datenintegrität
   - Provisioning
   - Self-Service
   - Synchronisierung der Anmeldeinfo
6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Installieren**.
8. Klicken Sie auf **Fertig stellen**.

Nach dem Abschluss des Installationsassistenten wird der Assistent für die Dienstkonfiguration gestartet. Geben Sie die Konfigurationsinformationen für den Dienst an, z. B. Verbindungseinstellungen, Zertifikatsname, Name und Kennwort für das Dienstkonto und den Speicherort des zentralen Speichers. Weitere Informationen finden Sie unter „So konfigurieren Sie die Password Manager-Dienste“ auf Seite 108.

Schritt 2: Aktualisieren der Password Manager Console

Die Konsole, mit der Sie die Password Manager 4.1- oder 4.5-Umgebung verwalten, wird deinstalliert, wenn Sie die Konsole für Password Manager 4.6 installieren. Sie sollten alle installierten Konsolen und das Anwendungsdefinitionstool aktualisieren.

Wichtig: Bei der ersten Durchführung und Konfiguration der Discovery in der Konsole für Password Manager 4.6 können Sie den zentralen Speicher (und die Daten im zentralen Speicher) aktualisieren. Aktualisierte Versionen des zentralen Speichers sind nicht mit älteren Versionen der Konsole kompatibel. Weitere Informationen finden Sie unter „Sichern des vorhandenen zentralen Speichers“ auf Seite 138.

Wenn der Dienst und die Konsole auf demselben Computer installiert sind, müssen beide aktualisiert werden.

Weitere Informationen finden Sie auch unter „Microsoft .NET Version 1.1 und 2.0“ auf Seite 140.

So aktualisieren Sie die Password Manager Console

1. Klicken Sie auf **Schritt 3: Administrative Komponenten installieren**.
2. Klicken Sie auf **Schritt 3: Password Manager Console installieren**.
3. Klicken Sie auf **Weiter**, stimmen Sie der Lizenzvereinbarung zu und klicken Sie erneut auf **Weiter**.

   Die Seite **Aktualisieren der Citrix Password Manager Console** wird angezeigt.
4. **Nur für ein Upgrade von Version 4.1:** Klicken Sie auf **Weiter**, um das Entfernen der vorhandenen Version der Konsole zu bestätigen und die Installation fortzusetzen.

   Das Dialogfeld **Installationstyp** wird angezeigt.

5. Wählen Sie die zu installierenden Komponenten aus und klicken Sie auf **Weiter**.

Konsole	Aktivieren Sie diese Option, um die Konsole zu installieren. Diese wird benötigt, um Richtlinien, Anwendungsdefinitionen, Benutzerkonfigurationen usw. zu erstellen und zu verwalten.
Anwendungs-definitionstool	Aktivieren Sie diese Option, um das Tool zu installieren, mit dem Sie Anwendungsdefinitionen erstellen können, ohne die Konsole zu starten oder zu verwenden. Auf Computern, auf denen die Konsole nicht installiert ist bzw. nicht installiert werden kann, können Sie dieses Tool im Standalone-Modus verwenden.
Lizenzserver-Administration	Aktivieren Sie diese Option, um diese Komponente zur Unterstützung der Lizenzverwaltung auf der Konsole zu installieren. Mit dieser Option können Sie eine Verknüpfung zum Lizenzserver erstellen.
Access Management Console - Diagnostic Facility	Aktivieren Sie diese Option, um den Citrix Support bei der Behebung von Problemen mit der Konsole zu unterstützen.

6. Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**, wenn die Installation abgeschlossen ist.
7. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.

   Bei der Konfiguration und Durchführung der Discovery werden Sie in einem Dialogfeld gefragt, ob Sie zu diesem Zeitpunkt den zentralen Speicher aktualisieren möchten.
8. Klicken Sie auf **Ja**.

9. **Nur für ein Upgrade von Version 4.1:** Klicken Sie auf **Upgrade**.

   Hinweis: Wenn Sie auf **Kein Upgrade** klicken, müssen Sie die Discovery jedes Mal mit der Konsole konfigurieren und durchführen, bis Sie das Upgrade vornehmen. (Beenden Sie dazu die Konsole, starten Sie sie neu und klicken Sie auf **Upgrade**.) Wenn Sie auf **Kein Upgrade** klicken, können Sie keine Einstellungen oder Ergebnisse der angezeigten Discovery in der Konsole speichern.

10. Konfigurieren Sie die Konsole wie unter „So konfigurieren Sie die Password Manager Console“ auf Seite 115 beschrieben.

Hinweis: Wenn Sie die Discovery danach im Rahmen des Upgradeprozesses mit der Konsole der Version 4.6 konfigurieren und durchführen und Sie als zentralen Speicher eine NTFS-Netzwerkfreigabe verwenden, werden Sie aufgefordert, den zentralen Speicher zu aktualisieren. Klicken Sie auf **OK**, um das Upgrade durchzuführen, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen. Wenn Sie den zentralen Speicher an dieser Stelle nicht aktualisieren, können Sie nur die früheren Versionen (4.1 und 4.5) der Konsole zusammen mit dem zentralen Speicher verwenden.

Schritt 3: Aktualisieren von Password Manager Agent

Hinweis: Wenn Sie den Password Manager-Dienst und die Password Manager Console, jedoch nicht die Agentsoftware aktualisieren, können Benutzer, deren Benutzerkonfigurationen mit Active Directory-Hierarchien (Organisationseinheiten oder Benutzer) verknüpft sind, dennoch die grundlegenden Funktionen der Agentsoftware verwenden. Jedoch haben die Benutzer dann keinen Zugriff auf die aktuellen Funktionen von Password Manager. Citrix empfiehlt, die Agentsoftware möglichst zu aktualisieren, damit sie mit den Versionen des Dienstes und der Konsole übereinstimmt.

Die vorhandene Agentsoftware wird entfernt, wenn Sie die Agentsoftware für Password Manager 4.6 installieren.

So führen Sie ein Upgrade von Password Manager Agent auf einem lokalen Client durch

Hinweis: Wenn Sie im Rahmen der Agentinstallation Hotdesktop in der Umgebung einsetzen möchten, lesen Sie die Informationen unter „Benutzererfahrung bei Hotdesktop“ auf Seite 52.

Bei den folgenden Schritten wird davon ausgegangen, dass die Password Manager-CD in den Computer eingelegt ist, auf dem die Agentsoftware installiert wird, und dass das Autorun-Dialogfeld angezeigt wird.

1. Klicken Sie auf **Schritt 4: Password Manager Agent-Software installieren.**
2. Klicken Sie auf **Password Manager Agent installieren**.

   Das Dialogfeld **Upgradeerkennung** wird angezeigt.
3. Klicken Sie im Bestätigungsdialogfeld auf **Ja**, um die vorherige Version des Dienstes zu entfernen und die Installation fortzusetzen.

   Der **Installationsassistent von Password Manager Agent** wird angezeigt.
4. Klicken Sie auf **Weiter**, stimmen Sie der Lizenzvereinbarung zu und klicken Sie erneut auf **Weiter**.

   Das Dialogfeld **Funktionsauswahl** wird angezeigt.

5. Wählen Sie die optionalen Komponenten aus, die installiert werden, und klicken Sie auf **Weiter**.

   - Datenintegrität (wenn Sie diesen Dienst installiert haben)
   - Self-Service (wenn Sie diesen Dienst installiert haben)
   - Hotdesktop (für diese Option muss ein Konto zur Verwendung als Hotdesktop-Konto vorhanden sein)

     Hinweis: Hotdesktop wird nicht unter Windows Vista, allen Plattformen mit ausgeführten Terminaldiensten, allen Serverbetriebssystemen oder einem 64-Bit-Betriebssystem unterstützt

   - Java-Unterstützung (zur Installation der Password Manager-Unterstützung für die Java Runtime Environment (JRE), die bereits auf dem Client installiert ist)

   Das Dialogfeld **Zentralen Speicher konfigurieren** wird angezeigt.

6. Geben Sie auf der Seite **Zentralen Speicher konfigurieren** Folgendes an:

   A. Wählen Sie den Typ des zentralen Speichers.

   B. Prüfen Sie bei Auswahl von **NTFS-Netzwerkfreigabe** oder **Freigegebener Novell Ordner** den Speicherort des zentralen Speichers.

   C. Klicken Sie auf **Weiter**.

   Das Dialogfeld **Serveradresse angeben** wird angezeigt.

7. Prüfen Sie die Adresse und die Portnummer des Hostcomputers für den Dienst und klicken Sie auf **Weiter**.

   Geben Sie im Textfeld für die Adresse den vollqualifizierten Domänennamen des Dienstcomputers ein. Der Standardport ist 443.

   Wenn Sie Hotdesktop ausgewählt haben, wird das Dialogfeld **Hotdesktop-Konto konfigurieren** angezeigt.

   Hinweis: Wenn Sie Hotdesktop verwenden, dürfen weder Remotedesktop noch die Terminaldienste ausgeführt werden. Während der Hotdesktop-Installation setzt das Installationsprogramm den Wert des Registrierungsschlüssels **AllowMultipleSessions** auf 0 zurück.

8. Geben Sie die Anmeldeinformationen des Benutzers für das Hotdesktop-Konto ein und klicken Sie auf **Weiter**.

   Geben Sie den Namen der Domäne an, zu der die Arbeitsstation gehört. Verwenden Sie dabei den NetBIOS-Namen der Domäne und nicht den vollqualifizierten Domänennamen.

9. Klicken Sie auf **Installieren**.
10. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.
11. Führen Sie einen der folgenden Schritte aus:

    - Wenn Sie ein unterstütztes Betriebssystem außer Windows Vista verwenden, klicken Sie auf **Ja**, um das Clientgerät neu zu starten. Sie müssen das Clientgerät neu starten.
    - Unter Windows Vista müssen Sie sich vom Windows Vista-Konto ab- und dann erneut anmelden. Ein Neustart des Clientgeräts ist nicht erforderlich.